

Opinnäytetyö YAMK

Teknologiaosaamisen johtamisen koulutus

YTEJOS15

2020

Tapio Pulkkinen

TIETOVERKON KONFIGURAATIONHALLINNAN KEHITTÄMINEN JA TOIMINTA- TAPOJEN YHTENÄISTÄMINEN

Tapio Pulkkinen

TIETOVERKON KONFIGURAATIONHALLINNAN KEHITTÄMINEN JA TOIMINTATAPOJEN YHTENÄISTÄMINEN

Tietoverkko tarjoaa alustan ja mahdollistaa sähköisten IT-palveluiden tuottamisen, toimittamisen ja käytön. Palveluomaisuuden ja verkkolaitteiden konfiguraatietieto tulee saada mahdollisimman ketterästi prosessien ja eri rooleissa toimivien henkilöiden käyttöön.

Opinnäytetyössä selvitettiin miten palveluomaisuuden- ja konfiguraationhallintaa voidaan toiminnallisesti kehittää verkon teknisen ylläpidon ja palvelun häiriöttömän toiminnan varmistamiseksi. Tavoitteena oli löytää keinoja, kuinka voidaan yhtenäistää konfiguraationhallinnan toimintatapaa ja terävöittää konfiguraationhallinnan sekä eri tukiprosessien välistä yhteistoimintaa. Lisäksi tavoitteena oli löytää keinoja, kuinka voidaan parantaa konfiguraation rakenneosien tiedon saatavuutta.

Opinnäytetyö on laadultaan kvalitatiivinen tutkimus. Tutkimusmetodeja olivat kirjallisuustutkimus ja käytännön osuuden teemahaastattelut. Haastatteluun valittiin asiantuntijoita, joilla oli laaja-alainen ja vuosien kokemus toimialan eri tehtävistä.

Tutkimuksen tuloksena tunnistettiin ja raportoitiin palveluomaisuuden- ja konfiguraationhallinnan merkitys sekä vaikuttavuus suhteessa palvelutuotannon muihin käytäntöihin. Lisäksi työ tuotti kehittämis ehdotuksia ja tietoa kehittämistyön sekä toimintatapojen yhtenäistämisen tueksi. Tutkimuksessa todetut keskeisimmät kehittämisalueet liittyvät konfiguraationhallinnan ja eri tukiprosessien väliseen yhteistoimintaan sekä yhteiskäyttöisen konfiguraatietiedon saatavuuteen.

Tutkimuksessa havaittiin, että toimiva muutoksenhallinta on konfiguraationhallinnan yksi tärkeimmistä tukiprosesseista. Muutoksenhallinta kontrolloi, että verkkolaitteen rakenneosatiedon muutokset tehdään ja dokumentoidaan hallitusti laitteen elinkaaren kaikissa vaiheissa. Lisäksi havaittiin, että tiedonhallinnan eri osa-alueiden keskinäinen yhteistoiminta ja tasapaino vaikuttavat merkittävästi palveluomaisuuden- ja konfiguraationhallinnan suorituskykyyn.

ASIASANAT:

Tietoverkko, konfiguraationhallinta, konfiguraation rakenneosa, ITIL

Tapio Pulkkinen

DEVELOPMENT OF THE NETWORK CONFIGURATION MANAGEMENT AND HARMONIZATION OF POLICIES

Information and communication networks provide a platform and enable the production, delivery and use of electronic IT services. The configuration data of the service assets and network devices must be made available to processes and people in different roles as effortlessly as possible.

The present Master's thesis focuses on how the service asset management and configuration management can be developed functionally to ensure the technical maintenance of the network and operation of the service without disruptions. The aim was to find ways to unify the procedures of the configuration management and to enhance the collaboration between configuration management and different support processes. In addition, the goal was to identify ways to improve the availability of the information about configuration items.

This thesis is a qualitative research. The research methods used were literature research and thematic interviews which were included in the practical part. The interviewees selected for the interviews had years of wide experience in various tasks in the industry.

As a result of the study, the importance and effectiveness of service asset and configuration management in relation to other service production practices were identified and reported. In addition, the study produced development proposals and information to support development work and the harmonization of operating methods. The main development areas identified in the study are related to the collaboration between configuration management and different support processes, as well as to the availability of shared configuration information.

The results of the study indicate that effective change management is one of the most important support processes for configuration management. Change management monitors that the changes of the network device component information are made and documented in a controlled manner at all stages of the device lifecycle. In addition the study shows that the collaboration and balance between the different areas of information management significantly affect the performance of service asset and configuration management.

KEYWORDS:

Network, configuration management, configuration item, ITIL

SISÄLTÖ

KÄYTETYT LYHENTEET	6
1 JOHDANTO	7
1.1 Taustaa	7
1.2 Tarkoitus ja tavoitteet	8
2 PERUSTEITA KONFIGURAATIONHALLINTAAN	10
2.1 Tietoliikenneverkko	10
2.2 Vahti sisäverkko-ohjeen vaatimuksia	12
2.3 Palvelunhallinnan standardi ja parhaita käytäntöjä	14
3 PALVELUOMAISUUDEN- JA KONFIGURAATIONHALLINTA	22
3.1 Peruskäsitteet	23
3.2 Tiedonhallinta	24
3.3 Palvelutietämyksen hallintajärjestelmä	26
3.4 Palveluomaisuuden- ja konfiguraationhallintaprosessin aktiviteetit	29
3.5 Konfiguraation rakenneosan elinkaarenhallinta	30
3.6 Rajapinnat prosessien välillä	31
4 TEEMAHAASTattelun toteutus ja tulokset	36
4.1 Teemahaastattelun osallistujat ja haastattelujen toteutus	36
4.2 Konfiguraation tunnistamisen tulosten käsittely	37
4.3 Konfiguraation kontrollin tulosten käsittely	39
4.4 Tilan seurannan ja raportoinnin tulosten käsittely	41
4.5 Prosessien ja roolien tulosten käsittely	42
4.6 Yhteenveto ja päätelmät teemahaastattelun tuloksista	44
4.7 Luotettavuuden arviointi	46
5 EHDOTETUT KEHITTÄMISTOIMENPITEET	49
LÄHTEET	54

LIITTEET

Liite 1. Teemahaastattelun kysymysrunko

KUVAT

Kuva 1. Yleisimmät verkkotopologiat (mukaillen Beasley & Nilkaew 2012, 7, 11).	10
Kuva 2. Hierarkkisen lähiverkon rakenne (Cisco Networking Academy 2018, 7).	11
Kuva 3. Palvelunhallintajärjestelmä (SFS-ISO/IEC 20000-1:2018, 7).	16
Kuva 4. ITIL 3 elinkaarimalli (mukaillen ITIL Service Strategy 2011, 3).	17
Kuva 5. ITIL 4 palvelun arvojärjestelmä (ITIL Foundation 2019, 3).	19
Kuva 6. ITIL 4 palvelunhallinnan neljä ulottuvuutta (ITIL Foundation 2019, 25).	20
Kuva 7. Tiedonhallinnan suunnittelun viitekehys (Kaario & Peltola 2008, 137).	25
Kuva 8. Palvelutietämyksen hallintajärjestelmä (ITIL Perustason käsikirja 2013, 208).	27
Kuva 9. Konfiguraationhallintajärjestelmän tasot (Shirley & Norfolk 2014, 4).	28
Kuva 10. Palveluomaisuuden- ja konfiguraationhallinta (Bon van 2009, 114).	29
Kuva 11. Konfiguraation rakenneosan elinkaarenhallinta (mukaillen BMC Software 2016, 150).	30
Kuva 12. Erään yrityksen prosessirajapintoja (mukaillen Drogseth ym. 2015, 40).	32
Kuva 13. Muutoksenhallinnan sekä palveluomaisuuden- ja konfiguraationhallinnan välinen rajapinta (mukaillen ITIL Service Strategy 2011, 87).	34

TAULUKOT

Taulukko 1. Verkon tietoturva vaatimuksia (VAHTI johtoryhmä 2010, 29).	14
Taulukko 2. Tietoverkon tai laitteen konfiguraation rakenneosan (CI) attribuutteja.	38

KÄYTETYT LYHENTEET

Lyhenne	Lyhenteen selitys
CAB	Change Advisor Board
CI	Configuration Item
CMDB	Configuration Management Database
CMS	Configuration Management System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT service management
LAN	Local Area Network
SACM	Service Asset Configuration Management
SFS	Finnish Standards Association SFS
SDN	Software Defined Networking
SKMS	Service Knowledge Management System
SMS	Service Management System
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
WAN	Wide Area Network

1 JOHDANTO

Yrityksen tai organisaation IT-infrastruktuuri on yksi tärkeistä liiketoiminnan kivijaloista. Infrastruktuurin muodostaa tieto- ja tietoliikenneverkoista koostuva palveluomaisuus, joka tarjoaa alustan ja mahdollistaa sähköisten palveluiden tuottamisen, toimittamisen ja käytön. Usein palvelut hankitaan avaimet käteen periaatteella verkko- ja palveluoperaattoreilta. Sopimuksesta riippuen operaattori voi omistaa verkkoinfran ja päätelaitteet ovat yrityksen omistuksessa. Määräys yleisten viestintäverkkojen ja -palvelujen varmistamisesta asettaa operaattorille tai teleyritykselle minimivelvoitteita muun muassa palvelujen toteutuksessa käytettävien laitteiden ja yhteyksien varmentamiselle, laitteiden suojaamiselle sekä viestintäverkkojen synkronoinnille. Määräyksen tavoitteena on varmistaa viestintäpalveluiden toimivuus myös häiriötilanteissa. Viestintäverkon tai – palvelun komponentilla tarkoitetaan verkkoelementtiä, laitetta tai järjestelmää. (Viestintävirasto 54 B/2014 M.)

Palvelun liiketoimintakriittisyys määrittää IT-palvelun saatavuustavoitteen. Saatavuudella (availability) tarkoitetaan ajanjaksoa, jolloin palvelu on käytettävissä palveluaikana. Katkos palvelussa sovittuna palveluaikana laskee palvelun saatavuutta. Saatavuus ilmoitetaan prosenttilukuna palveluajasta. Esimerkiksi 99%:n saatavuus tarkoittaa, että palvelu on poissa käytöstä enintään neljätoista minuuttia päivässä. Mitä korkeampi on palvelun saatavuus, sitä korkeammat ovat palvelun kustannukset. Korkean saatavuuden palvelu edellyttää vikasietoista tietoverkkoa ja asettaa vaatimuksia verkon ylläpitokäytännöille. (Julkisen hallinnon tietohallinnon neuvottelukunta 2019, 24-25.)

1.1 Taustaa

Konfiguraationhallinta on yksi verkon ylläpidon käytännöistä, jonka tehtävänä on omalta osaltaan varmistaa sovitun saatavuustavoitteen toteutuminen. Lisäksi käytäntö huolehtii, että palveluomaisuutta kyetään hallitsemaan oikealla tavalla. Konfiguraationhallintaan liittyy tietoa ja tietämystä, joita tarvitaan verkkojen suunnitteluun, verkkolaitteiden käyttöönottoon, ylläpitoon ja käytöstä poistoon. Ylläpitoa ovat muun muassa herätteiden hallinta, häiriönhallintaan liittyvä viankorjaus ja konfiguraatiomuutokset verkkolaitteiden elinkaaren eri vaiheissa. Tieto- ja tietoliikenneverkkojen sekä niiden verkkolaitteisiin liittyvä

tietämys ja konfiguraatietieto tulisi olla luotettavaa, ajantasaista ja tarvitsijoiden saatavilla. Ylläpidon haasteita lisää palveluiden monitoimittajaympäristö, automaattisesti ja manuaalisesti ylläpidettävä tiedon määrä ja sirpaleisuus.

Konfiguraationhallintaa voidaan toteuttaa laadukkaasti eri tavoin. Lähtökohtana on yrityksen tai organisaation tarpeet ja painopistealueet. Käytännön kokemuksia, alan kirjallisuutta, standardeja ja viitekehyksiä hyödyntäen on mahdollista räätälöidä toimiva ja IT-palvelutuotantoa tukeva konfiguraationhallinnan kokonaisuus. Yleisesti käytetty ITIL-viitekehys (Information Technology Infrastructure Library) tarjoaa järjestelmällisen lähestymistavan laadukkaiden IT-palveluiden tuottamiseen. Viitekehyksen mukaan palveluomaisuuden – ja konfiguraationhallinta (SACM, Service Asset Configuration Management) liittyy kaikkiin palvelun elinkaaren vaiheisiin. Tarkoituksena on hallinnoida palveluomaisuutta ja konfiguraation rakenneosia (CI, Configuration item) sekä tukea muita palvelunhallinnan prosesseja. (ITIL Perustason käsikirja 2013, 1, 175-176.)

Perinteiset tietoliikenneverkot pohjautuvat usein manuaalisesti konfiguroitaville valmistajakohtaisille ratkaisuille. Markkinoille on ilmestynyt viimeisten vuosien aikana uutta teknologiaa edustava ohjelmisto-ohjattu SDN-tekniikka eli Software Defined Networking. Ideana on, että verkon ja sen laitteiden käyttäytymistä kontrolloidaan, muutetaan ja hallinnoidaan keskitetysti jakamalla arkkitehtuuri omiin tasoihin (Ahmad 2018, 27). Tois-taiseksi tilanne on kuitenkin se, että monet nykyisistä SDN-ratkaisuista vaatii edelleen pohjalle perinteisen verkkotekniikan rakenteita.

1.2 Tarkoitus ja tavoitteet

Opinnäytetyön tarkoituksena on selvittää, miten tietoverkon verkkolaitteiden palveluomaisuuden- ja konfiguraationhallintaa voidaan toiminnallisesti kehittää teknisen ylläpidon ja palveluiden häiriöttömän toiminnan varmistamiseksi.

Opinnäytetyön tavoitteena on löytää keinoja, kuinka voidaan yhtenäistää konfiguraationhallinnan toimintatapaa, terävöittää konfiguraationhallinnan ja eri tukiprosessien välistä yhteistoimintaa sekä parantaa yhteiskäyttöisen konfiguraatietiedon saatavuutta. Opinnäytetyö tuottaa organisaatioriippumatonta yleispätevää ja myös käytännönläheistä tietoa sekä materiaalia kehittämistyön tueksi. Työ tarjoaa myös näkemyksiä siitä, miten konfiguraationhallintaa kannattaa kehittää vastaamaan tulevaisuuden tarpeita.

Tutkimus koskee verkon valvonnan ja hallinnan piirissä olevia tietoverkkojen verkkolaitteita. Ohjelmisto-ohjattu SDN-tekniikka ei sisälly tutkimuksen kehykseen. Tutkimusotteena käytetään kvalitatiivista menetelmää. Aineisto hankitaan teemahaastatteluilla ja analysointiin käytetään osaltaan diskurssianalyysin menetelmää. Työssä sovelletaan olemassa olevaa teoriaa kirjallista lähdemateriaalia tutkimalla. Lisäksi tutkija hyödyntää tutkimuksessa omaa tietotekniikka-alan yleistä kokemusta ja konfiguraationhallinnan kurssilta saatuja oppeja.

Palveluomaisuuden- ja konfiguraationhallinta on IT-organisaation palvelunhallintajärjestelmän yksi erityisosaamista vaativa kokonaisuus, joka sisältää useita rajapintoja palvelunhallinnan muihin käytäntöihin. Tutkimuksessa käsitellään muun muassa konfiguraationhallinnan toimintatapaa, merkitystä ja vaikuttavuutta palveluiden hallintaan. Työn kokonaisuuden keskeisimpiä aihealueita ovat verkkolaitteen konfiguraation rakenneosien (CI) elinkaaren- ja tiedonhallinta palvelutuotannon prosesseissa sekä prosessirajapintojen yli. Näiden osalta muita aihealueita ovat tietojen hallintaan käytettävä konfiguraationhallintajärjestelmä (CMS, Configuration Management System) sekä tietoliikenneverkkojen rakenne ja niiden tietoturva.

Palveluomaisuuden- ja konfiguraationhallinnan käytäntöjä tarkastellaan erityisesti ITIL-viitekehystä vasten, koska työn toimeksiantaja Puolustusvoimien johtamisjärjestelmäkeskus soveltaa viitekehyksen periaatteita palvelutuotannon tukiprosesseissa. Pääesikunnan alaisena laitoksena Puolustusvoimien johtamisjärjestelmäkeskus mahdollistaa puolustusvoimien johtamisen järjestämällä tietotekniset palvelut yhteistoiminnassa kumppaneiden kanssa. Keskuksen päätehtäviin kuuluu myös kyberpuolustus. Puolustusvoimien johtamisjärjestelmäkeskus toimii usealla paikkakunnalla ympäri Suomen. (Puolustusvoimat, 2020.)

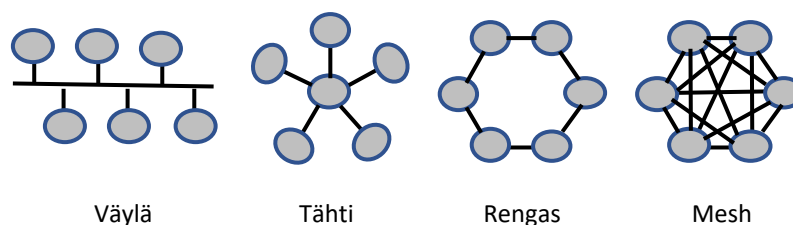
2 PERUSTEITA KONFIGURAATIONHALLINTAAN

2.1 Tietoliikenneverkko

Tietoliikenneverkko tarjoaa alustan ja mahdollistaa sähköisten IT-palveluiden tuottamisen, toimittamisen ja käytön. Niin julkinen sektori, yritykset kuin tavalliset kansalaisetkin ovat riippuvaisia verkkojen kautta tarjottavista palveluista. Verkko muodostuu solmupisteistä ja niiden välisistä yhteyksistä. Solmupisteiden tyypillisiä verkkolaitteita ovat kytkin, reitin, palomuuuri tai langaton tukiasema. Tyypillisiä verkkoon kiinteästi tai langattomasti kytkettäviä päätelaitteita ovat tietokone, IP-puhelin ja tulostin.

Verkkotopologia

Topologia on verkkoarkkitehtuuri, jota käytetään verkkolaitteiden yhdistämiseen. Yleisimmät lähiverkkojen (LAN, Local Area Network) topologiat ovat rengas-, väylä-, tähti- ja mesh-topologiat. Fyysinen topologia kuvaa verkon toteuttamiseen käytettyjen laitteiden järjestelyn, kuva 1. (Beasley & Nilkaew 2012, 7-11.)



Kuva 1. Yleisimmät verkkotopologiat (mukaillen Beasley & Nilkaew 2012, 7, 11).

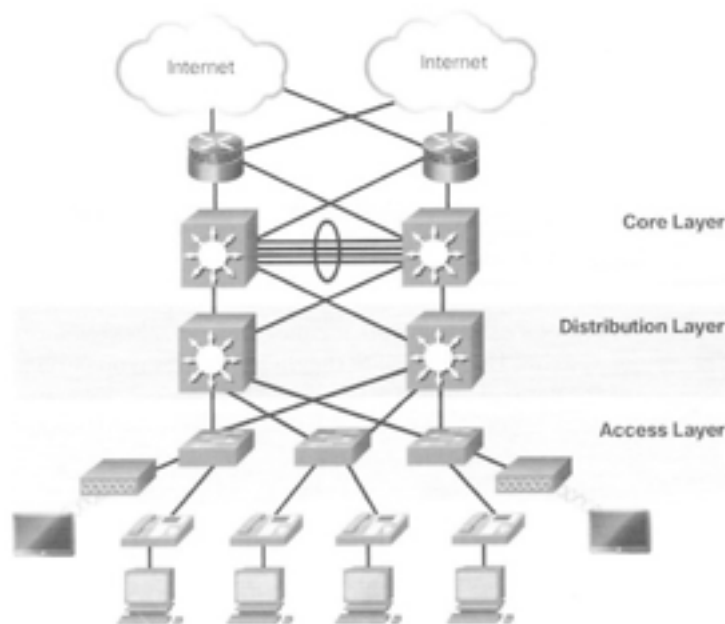
Verkkotopologian valinnassa tulee kiinnittää huomiota verkon modulaarisuuteen, skaalautuvuuteen, joustavuuteen ja hallintaan unohtamatta verkon muuta ylläpitoa. Esimerkiksi silmukoitu mesh-verkko on vikasietoinen, mutta vaatii muutoksissa enemmän verkkolaitteiden konfigurointia ja konfiguraatitiedon ylläpitotyötä. Mahdollinen verkon ja toimintojen automatisointi helpottaa osaltaan konfiguraatiohallintaa.

Lähiverkolla tarkoitetaan verkkoa, joka mahdollistaa tiedonsiirron verkkolaitteiden välillä ja tarjoaa loppukäyttäjille pääsyn verkon tietoliikennepalveluihin ja resursseihin. Yrityksen maantieteellisesti rajattuun kampusverkkoon voidaan liittää useita lähiverkkoja.

Kampuksella tarkoitetaan tässä yhteydessä yhtä tai useampaa rakennusta samalla alueella. Lähiverkko mahdollistaa tiedonsiirron rakennusalueen laitteiden välillä ja verkkoyhteydet laajaverkon (WAN, Wide Area Network) tai internetin kautta maantieteellisesti toisessa kaupungissa tai toisella puolella maapalloa olevaan saman yrityksen kampuslähiverkkoon. Yrityksen liiketoiminnan laajentuminen tai supistuminen asettaa vaatimuksia erityisesti verkon skaalautuvuudelle. (Cisco Networking Academy 2018, 3-6.)

Hierarkkinen tietoliikenneverkko

Hierarkkisella tietoliikenneverkolla tarkoitetaan rakennetta, jossa verkko on jaettu toiminnallisiin tasoihin. Hierarkkinen rakenne yksinkertaistaa verkon suunnittelua, käyttöönottoa ja ylläpitoa sekä parantaa verkon modulaarisuutta, skaalautuvuutta, joustavuutta ja hallintaa. Hierarkkinen lähiverkkoverkko muodostuu kuvan 2 mukaisesti liityntäverkosta (engl. access layer), jakeluverkosta (engl. distribution layer) ja runkoverkosta (engl. core layer). (Cisco Networking Academy 2018, 6-7.)



Kuva 2. Hierarkkisen lähiverkon rakenne (Cisco Networking Academy 2018, 7).

Liityntäverkko mahdollistaa loppukäyttäjän pääsyn verkon tarjoamiin palveluihin ja toimintoihin. Liityntäverkkoon kytkettäviä langallisia päätelaitteita ovat esimerkiksi tietokone, IP-puhelin, tulostin tai langaton tukiasema. Etätyöntekijöille voidaan tarjota pääsy

yrittäverkkoon laajaverkon (WAN) teknologioiden tai internetin kautta. Kyvykkään liityntäverkon ominaisuuksia ovat korkea saatavuus, vikasietoisuus ja perustason tietoturva. (Froom & Frahim 2015, 11-12.)

Jakeluverkko kokoaa liityntäverkon päätelaitteilta tulevan datan ja toimii reitittävänä rajapintana liityntäverkon ja runkoverkon välillä. Korkea käytettävyyys on jakeluverkon tärkeä ja suunnittelussa huomioitava ominaisuus. (Froom & Frahim 2015, 12.)

Runkoverkko kokoaa yhteen verkon kaikki elementit, yhdistää kampusverkot ja toimii rajapintana verkon tarjoamiin palveluihin ja ulkoiseen laajaverkkoon. Runkoverkolta odotetaan korkeaa käytettävyyttä ja joustavuutta mahdollistaen esimerkiksi ohjelmisto- ja laitepäivitykset ilman palvelukatkoksia. Tästä johtuen runkoverkon verkkokäytännöt ja -konfiguraatiot pyritään pitämään yksinkertaisina ilman monimutkaisia toimintoja ja suoria yhteyksiä palvelimiin, tietokoneisiin tai muihin päätelaitteisiin. (Froom & Frahim 2015, 14-15.)

2.2 Vahti sisäverkko-ohjeen vaatimuksia

Vaatimuksenhallintaa tarvitaan minkä tahansa asian kehittämiseen. Vaatimuksenhallinta luo mahdollisuuden määritellä mitä ollaan tavoittelemassa ja mistä tekemisessä on kyse. Vaatimus kuvaa asiakkaan tahtoa liiketoiminnan, suorituskäyvyn, organisaation, tuotteen tai palvelun ominaisuuksiin. Vaatimuksenhallinta varmistaa, että vaatimukset kyetään keräämään kaikilta tarpeellisilta tahoilta sekä hallitsemaan luotettavasti organisaation prosesseissa. Toimiva vaatimuksenhallinta mahdollistaa toimintavapauden eri työvaiheille ja luo edellytykset kustannustehokkaille ratkaisuille. (Kosola 2013, 2.)

Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI julkaisi sisäverkko-ohjeen vuonna 2010. Ohjeen tavoitteena on yhtenäistää ja tehostaa menettelyitä sisäverkkojen rakentamisessa ja tukea sopivan tietoturvatason käyttöönottoa valtionhallinnon organisaatioissa. Ohjeessa on pyritty esittämään tuote- ja toimittajariippumattomasti verkkojen tietoturvallisuutta edistävät toimenpiteet.

Perinteisesti lähiverkon ymmärretään sijoittuvan pienelle alueelle joko yksittäiseen rakennukseen tai rakennusryhmään. Lähiverkon palveluiden etäkäyttö on lisääntynyt merkittävästi ja organisaatioilla saattaa olla useita toimipisteitä eri paikkakunnilla. Verkkoarkkitehtonisesti toimipisteet ovat usein yhtä ja samaa verkkoa. Sisäverkko-ohjeen tar-

koitusta varten lähiverkko on laajennettu käsittämään koko organisaation loogisen tietoverkon. Siksi lähiverkko-termin sijaan ohjeessa puhutaan organisaation sisäisestä tietoverkosta, lyhyemmin sisäverkosta. (Valtion tietoturvallisuuden johtoryhmä 2010, 19.)

Verkon rakenteen mukaiset tiedon suojaustasot

Sisäverkko-ohjeen mukaan verkot jaetaan verkkorakenteen mukaan perus-, korotetun ja korkean tason verkkoihin. Tietoverkossa käsiteltävät tiedot luokitellaan suojaustasoihin ST I – ST IV. Suojaustason IV tietoa voidaan käsitellä perustason verkoissa. Korotetun tason verkossa voidaan käsitellä suojaustason III tietoa salaamattomana, mikäli kaikki verkkotasolle asetetut vaatimukset täyttyvät. Valtionhallinnon toimistoverkot ovat tyypillisesti perustason verkkoja.

Perus- ja korotetun tason verkkoja on mahdollista kytkeä internettiin ja muihin ei-luotettuihin verkkoihin mikäli kyseisen verkkotason vaatimukset täyttyvät. Korkean tason verkot ovat fyysisesti muista verkoista eristetty. Toimivaltainen viranomainen voi tapauskohtaisesti hyväksyä korkean tason verkon kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon. Korkean tason verkot mahdollistavat suojaustason II tietojen käsittelyn salaamattomana. (Valtion tietoturvallisuuden johtoryhmä 2010, 34.)

Vuoden 2020 alusta suojaustasomerkintöjen lyhenteet ovat muuttuneet. Suojaustason lyhenne ST I – ST IV kirjataan uuden suosituksen mukaan turvallisuusluokituksen merkinnällä TL I – TL IV. (Valtionvarainministeriön julkaisuja 2020:19, 10).

Verkon eri tasojen tietoturvavaatimuksia

Sisäverkko-ohje kuvaa verkon tasot palvelukeskeisen ajattelumallin mukaan kolmeen tasoon. Alimmalla tasolla ovat päätelaitteet ja verkon aktiivilaitteet. Keskimmaisella tasolla verkon arkkitehtuurin mukainen rakenne ja tietoliikenne. Ylimmällä tasolla palvelut ja palvelujen käyttäjät. Tietoturvan näkökulmasta verkon tulee täyttää vähintään taulukon 1 mukaiset vaatimukset.

Taulukko 1. Verkon tietoturva-vaatimuksia (VAHTI johtoryhmä 2010, 29).

Vaatus	Kuvas
Luottamuksellisuus (engl. confidentiality)	Tieto on vain valtuutettujen käyttäjien ulottuvilla.
Eheys (engl. integrity)	Tieto on vain valtuutettujen käyttäjien muokattavissa, eikä tieto muutu hallitsemattomasti.
Saatavuus (engl. availability)	Tieto on valtuutettujen käyttäjien saatavilla, kun he sitä tarvitsevat.

Palvelukeskeisessä mallissa palveluiden saatavuus turvataan erilaisilla kahdennusratkaisulla. Verkon eri tasojen luottamuksellisuus ja eheys voidaan varmistaa käyttäjänhallinnalla, salauksella ja lokituksella sekä laittilojen fyysisellä suojauksella.

Päätelaitteiden osalta saatavuus ei ole erityisen kriittinen vaatimus mikäli palvelu toimii kokonaisuudessaan verkossa. Palveluiden saatavuus varmistetaan varalaittejärjestelyillä. Lisäksi tietoa voidaan tilapäisratkaisuna tallentaa työasemalle tai erilliselle tallennusmedialle. Tietojen tallentamista verkkopalvelujen ulkopuolelle ei kuitenkaan suositella.

Kahdennuksilla ja varmennetulla virransyötöllä varmistetaan verkon aktiivilaitteiden saatavuus. Aktiivilaitteita ovat kytkimet, reitittimet ja vastaavat laitteet. Lisäksi voidaan käyttää komponentteja, jotka mahdollistavat niiden poistamisen ja korvaamisen laitteen ollessa päällä. Verkon arkkitehtuurin ja rakenteen saatavuus varmistetaan vikasietoisilla teknologiavalinnoilla ja varmentamalla kriittiset yhteydet.

Tietoliikenne on verkkoon kytkettyjen laitteiden välistä vuorovaikutusta. Tietoliikenteen protokollavalinnoilla varmistetaan saatavuus ja erilaisilla salausratkaisulla luottamuksellisuus. Eheys varmistetaan tunnistamalla osapuolet ennen kommunikoinnin aloittamista. (Valtion tietoturvasuuden johtoryhmä 2010, 30-31.)

2.3 Palvelunhallinnan standardi ja parhaita käytäntöjä

ITIL on viitekehys ja kokoelma palvelunhallinnan parhaita käytäntöjä (ITSM, IT service management) tarjoamalla järjestelmällisen lähestymistavan laadukkaiden IT-palveluiden tuottamiseen. Parhaat käytännöt auttavat organisaatiota saavuttamaan standardin ISO/IEC 20000 valtuutuksen ja sertifiointin. Tavoitteen saavuttamista tukee laadun ja vertailtavuuden näkökulma. ITIL on käytössä tai sitä hyödynnetään tuhansissa organisaatioissa ympäri maailmaa. (ITIL Service Strategy 2011, 3.) Käytännössä standardi ja ITIL viitekehys on keskenään yhteensovitettu. Viitekehys on toimittajariippumaton.

ISO/IEC 20000

IT-palvelunhallinnan standardin keskeisiltä osiltaan uudistunut painos julkaistiin joulukuussa 2018. Standardi soveltuu sekä sisäisille että ulkoisille palveluntuottajille. Painoksessa otetaan huomioon erityisesti nousussa olevat kehityssuunnat, kuten palveluiden mieltäminen hyödykkeiksi, useampien toimittajien hallinta sisäisen tai ulkoisen palveluintegraattorin toimesta sekä tarve määrittää palveluista asiakkaille syntyvä arvo. Uusia ominaisuuksia ovat tietämystä ja palveluiden suunnittelua koskevat vaatimukset. Lisäksi dokumentoinnin vaatimuksia muutettiin tai kevennettiin. Esimerkiksi konfiguraatietietokantaa koskeva vaatimus korvattiin konfiguraatietietoa koskevilla vaatimuksilla. (SFS-ISO/IEC 20000-1:2018, 4-5.)

Standardisarja sisältää kahdeksan osaa, joista neljään luodaan yleiskatsaus tässä yhteydessä. Standardin ensimmäinen osa on keskeinen ja tärkein, jota kaikki muut osat täydentävät ja tukevat. Standardi määrittää palvelunhallintajärjestelmää (SMS, Service Management System) koskevat vaatimukset. Toinen osa antaa ohjeistusta palvelunhallintajärjestelmän toteuttamiseen. Käytännössä ohjeet ovat esimerkkejä ja ehdotuksia, joiden avulla organisaatiot kykenevät tulkitsemaan standardin ensimmäistä osaa ja toiminaan sen mukaisesti. Standardisarjan yhteisen viitekehyksen luo osa kymmenen, joka kuvaa kaikkien osien tarkoituksen ja niiden väliset suhteet. Standardi on myös määräävä lähde termeille ja määritelmille, joita käytetään standardisarjan kaikissa osissa. Sarjan yhdestoista osa on tekninen raportti, joka antaa ohjeistusta standardin ensimmäisen osan ja yleisesti käytetyn ITIL-viitekehyksen välisestä suhteesta. Viitekehys on perustuu palvelun elinkaarimalliin. Standardisarjan ulkoisia vaikuttimia ovat viitekehykset ja hyvät käytännöt, toimialakohtaiset standardit, kansalliset standardit ja kansainväliset standardit. (SFS-ISO/IEC 20000-2:2014, 8; 20000-10:2018, 7, 27.)

Palvelunhallintajärjestelmälle (SMS) asetetut vaatimukset koskevat järjestelmän laatimista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista. Järjestelmä tukee elinkaaren hallintaa täyttämällä sovitut vaatimukset ja tuottamalla arvoa asiakkaille, käyttäjille ja palvelua toimittavalle organisaatiolle. Palvelunhallintajärjestelmää voidaan tukea käyttötarkoitukseen soveltuvilla palvelunhallinnan työkaluilla. Standardi ei vaadi minkään tietyn ohjeistuksen noudattamista vaan palvelutuotanto- tai asiakasorganisaatiot voivat vapaasti yhdistellä yleisesti hyväksytyjä viitekehyksiä ja omaa kokemustaan. (SFS-ISO/IEC 20000-1:2018, 6.) Soveltamisen näkökulmasta tarkasteltuna standardin vaati-

mukset ovat yleisluonteisia sopien kaikkiin organisaatioihin niiden tyypistä, koosta tai toimitettavien palveluiden luonteesta riippumatta. Kaikki vaatimukset tulee kuitenkin huomioida mikäli organisaatio ilmoittaa noudattavansa standardia. (SFS-ISO/IEC 20000-1:2018, 8.)

Kuva 3 esittää palvelunhallintajärjestelmää (SMS, Service Management System) ilman rakenteellista hierarkiaa, järjestystä tai valtuutustasoja. Kuvan korostetut kohdat osoittavat esimerkkejä rajapinnoista ja integroinnin tarpeista konfiguraationhallinnan ja muun palvelunhallintajärjestelmän välillä.

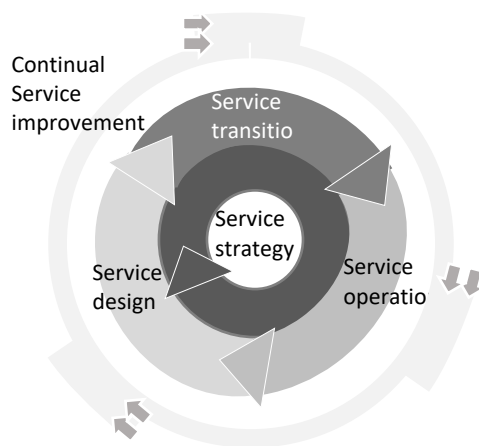


Kuva 3. Palvelunhallintajärjestelmä (SFS-ISO/IEC 20000-1:2018, 7).

Palvelunhallintajärjestelmä on johtamisen työkalu, joka sisältää palvelunhallinnan politiikat, tavoitteet, suunnitelmat, prosessit sekä dokumentoidun tiedon ja resurssit. Kaikki tämä vaaditaan palveluiden suunnitteluun, transiitioon, toimittamiseen ja parantamiseen sekä standardissa esitettyjen vaatimusten täyttämiseen. (SFS-ISO/IEC 20000-1:2018, 16.)

ITIL 3

ITIL:n kolmas päivitys julkaistiin vuonna 2011. Kuvan 4 mukaan julkaisu ottaa selkeän palvelunäkökulman jaottelemalla ydinprosessit palvelun elinkaarimallin mukaan palvelustrategiaan (engl. service strategy), palvelusuunnitteluun (engl. service design), palvelutransitioon (engl. service transition), palvelutuotantoon (engl. service operation) ja palvelun jatkuvaan parantamiseen (engl. continual service improvement). (ITIL Service Strategy 2011, 3.)



Kuva 4. ITIL 3 elinkaarimalli (mukaillen ITIL Service Strategy 2011, 3).

Kukin ydinprosessi sisältää aliprosesseja. Esimerkiksi palveluomaisuuden- ja konfiguraationhallinta on palvelutransitioon kuuluva prosessi, jolla on rajapintoja ja integraatioita muihin elinkaaren prosesseihin.

Palvelustrategia on palvelun elinkaaren ydin. Arvon luonti alkaa ymmärtämällä organisaation tavoitteet ja asiakkaan tarpeet. Palvelustrategia tarjoaa opastusta kuinka palvelunhallinta voidaan nähdä strategisena voimavarana eikä ainoastaan organisaation kyvykkyutenä. Strategiassa kuvataan ne periaatteet, jotka ovat hyödyllisiä kehitettäessä palvelunhallinnan politiikkaa, ohjeistusta ja prosesseja koko elinkaaren ajan. Palvelustrategian prosesseja ovat IT-palvelujen strategian hallinta, palveluportfolion hallinta, liiketoimintasuhteiden hallinta, kysynnän hallinta ja taloushallinta. (ITIL Service Strategy 2011, 5.)

Palvelusuunnittelun elinkaarivaiheessa palvelustrategia muutetaan suunnitelmaksi, jolla liiketoiminnan tavoitteet voidaan toteuttaa. Palvelusuunnittelu tarjoaa opastusta palvelui-

den ja palvelunhallinnan käytäntöjen suunnitteluun ja kehittämiseen. Se kattaa suunnitteluperiaatteet ja – menetelmät, joilla strategiset tavoitteet muutetaan palveluiksi ja palveluomaisuudeksi. Palvelun elinkaaren aikana hallinta tapahtuu palveluportfolion avulla sisältäen uudet, muuttuvat, kehitettävät ja parannettavat palvelut. Palvelusuunnittelun prosesseja ovat suunnittelun koordinointi, palveluluettelon hallinta, palvelutason hallinta, saatavuuden hallinta, kapasiteetin hallinta, IT-palvelun jatkuvuuden hallinta, tietoturvan hallinta ja toimittajahallinta. (ITIL Service Strategy 2011, 6.)

Palvelutransitio tarjoaa opastusta uusien ja muuttuneiden palveluiden viemiseksi tuotantoon. Se varmistaa, että palvelustrategiassa ja palvelusuunnittelussa tunnistetut arvot siirretään toteuttamiskelpoisina tehokkaasti tuotantoon. Lisäksi palvelutransitio opastaa palvelu- ja palveluhallintaprosessien muutoksenhallintaa pyrkien välttämään ei toivotut seuraukset jättäen kuitenkin tilaa innovaatiolle. Palvelutransition prosesseja ovat transition suunnittelu ja tuki, muutoksenhallinta, palveluomaisuuden- ja konfiguraationhallinta, jakelun- ja käyttöönoton hallinta, tietämyksenhallinta, palvelun validointi ja testaus sekä muutoksen evaluointi. (ITIL Service Strategy 2011, 6.)

Palvelutuotanto kuvaa parhaita palvelunhallinnan käytäntöjä palvelutuotannossa opastaen tehokkuuden ja vaikuttavuuden saavuttamiseen tuotannossa ja tuessa. Samalla se varmistaa arvon tuottamisen asiakkaalle, käyttäjälle ja palveluntuottajalle, opastaa vakauden ja jatkuvuuden ylläpidossa sekä tarjoaa prosessiohjeistusta, menettelytapoja ja työvälineitä reagoivasta ja ennakoivasta hallintanäkökulmasta. Lisäksi palvelutuotanto kerryttää tietoa ja tietämystä päätöksenteon parantamiseksi. Palvelutuotannon prosesseja ovat herätteiden hallinta, häiriönhallinta, ongelmanhallinta, palvelupyyntöprosessi ja pääsynhallinta. Palvelutuotantoon kuuluvia funktioita ovat palvelupiste, tekninen hallinta, IT-käyttöpalvelun hallinta ja sovellushallinta. (ITIL Service Strategy 2011, 6-7.)

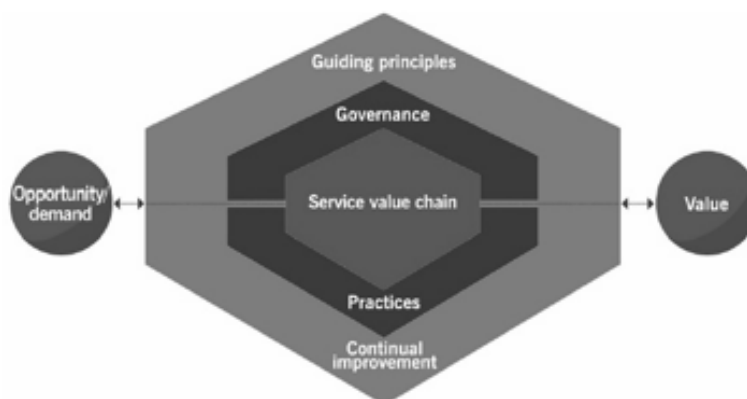
Palvelun jatkuva parantaminen tarjoaa opastusta arvon luomiseen ja ylläpitoon parantamalla palveluiden strategiaa, suunnittelua, transitiota ja tuotantoa. Se yhdistää laadunhallinnan, muutoksenhallinnan ja kyvykkyyksien parantamisen periaatteita, käytäntöjä ja menetelmiä. Lisäksi se kuvaa parhaita käytäntöjä parannusten saavuttamiseen ja varmistamiseen sekä tarjoaa jatkuvan palautemekanismin. Lähtökohtana on, että palveluportfolio on linjassa liiketoiminnan tarpeiden kanssa. Käytännössä palveluportfolio on kaikkien elinkaarivaiheiden ”selkäranka”. Palvelun jatkuvaan parantamiseen sisältyy myös palvelutason mittaus. (ITIL Service Strategy 2011, 7.)

ITIL 4

Palvelunhallinnan uusi viitekehys ITIL 4 julkaistiin vuoden 2019 alkupuolella. Päivitys on merkittävin vuoden 2011 version jälkeen. Uusi viitekehys ei kumoa eikä korvaa prosesseihin perustuvaa palvelun elinkaarimallia, mutta tuo lähes kymmenen vuotta tuoreempaa näkökulmaa ja ideoita palvelunhallintaan. Kuten päivitetty ISO 20000-standardi, myös ITIL 4 sisältää aikaisempaa vähemmän muodollisia vaatimuksia ja ottaa askeleen kohti yleistä palvelunhallintaa (Peltoniemi 2019.)

ITIL 3 tuottaa järjestystä kaaokseen muodon ja prosessien kautta. On kuitenkin huomattu, että asiakaskokemus, arvot, ideat ja ketteryys ovat jääneet muodon jalkoihin. Myös jatkuvan parantamisen mallin hyödyntäminen on jäänyt taustalle palvelunhallinnassa ja johtamisessa. Lisäksi teknologioiden kehittyminen ja digitaalinen murros tarjoaa jatkuvasti uusia vaihtoehtoja ja mahdollisuuksia. Murros johtaa väistämättä muutoksiin myös käytännön tekemisessä. Fyysisen infrastruktuurin korostamisen sijaan uudessa viitekehyksessä kiinnitetään enemmän huomiota esimerkiksi ohjelmistoihin ja niiden tuottamaan arvoon. Fyysisellä infrastruktuurilla eli ”raudalla” tarkoitetaan tässä yhteydessä muun muassa konesaliympäristöjä, palvelimia, verkkolaitteita ja työasemia. Edellä kuvattuihin asiakokonaisuuksiin ja haasteisiin ITIL 4 tarjoaa uusia ideoita ja käytäntöjä. (Peltoniemi 2019.)

Uusi viitekehys esittelee palvelunhallinnan ideat ja käytännöt osa-alueina, jotka muodostavat kuvan 5 mukaisen palvelun arvojärjestelmän (engl. service value system). Arvojärjestelmään kuuluu jatkuva parantaminen (engl. continual improvement), käytännöt eli kyvykkyudet (engl. practices), palveluiden hallintatapa (engl. governance) ja ohjaavat periaatteet (engl. guiding principles). (ITIL Foundation 2019, 3.)



Kuva 5. ITIL 4 palvelun arvojärjestelmä (ITIL Foundation 2019, 3).

Palvelun arvojärjestelmä toimii perusarkkitehtuurina käytännön tekemiselle, joka ottaa huomioon liiketoiminnan tarpeet ja arvot. Tekemisen ja jatkuvan parantamisen ytimessä on palvelun arvoketju (engl. service value chain) ja operatiivinen toimintatapa, joka jäsentää ja sitouttaa tekemistä. Syntyy kysyntää (engl. demand), palvelua toimitetaan ja toimitetulla palvelulla on arvojärjestelmän asiakkaalle tuottama arvo (engl. value). Arvojärjestelmän seitsemän ohjaavaa periaatetta ovat: Keskity arvoihin, aloita sieltä missä olet, kehitä ja paranna palaute huomioiden, edistä yhteistyötä ja näkyvyyttä, ajattele ja työskentele holistisesti, pidä käytännöt yksinkertaisina, optimoi ja automatisoi. (ITIL Foundation 2019, 3-4, 39.)

Palvelunhallinnan neljää ulottuvuutta esittää kuva 6. Keskiössä ovat tuotteet ja palvelut (engl. products and services), joilla on jokin arvo (engl. value). Ulottuvuuksia ovat organisaatiot ja ihmiset (engl. organizations and people), tieto ja teknologia (engl. information and technology), kumppanit ja toimittajat (engl. partners and suppliers) sekä arvovirrat ja prosessit (engl. value streams and processes). Jokaiseen ulottuvuuteen vaikuttaa ulkopuolisia tekijöitä, jotka voivat olla poliittisia (engl. political), taloudellisia (engl. economic), sosiaalisia (engl. social), teknologisia (engl. technological), oikeudellisia (engl. legal) tai ympäristöön (engl. environmental) liittyviä. (ITIL Foundation 2019, 25.)



Kuva 6. ITIL 4 palvelunhallinnan neljä ulottuvuutta (ITIL Foundation 2019, 25).

Viitekehys korostaa eri osapuolten aktiivisuutta. Näin syntyy enemmän hyötyä, jota voidaan jakaa. Asiakkaan ja toimittajan lisäksi mukana tulee olla myös kaikki sidosryhmät. Arvon tuottaminen pelkästään asiakkaalle ei johda kokonaisuuden kannalta parhaaseen lopputulokseen vaikka päärooleissa ovatkin asiakas ja toimittaja. (Peltoniemi 2019.)

ITIL 4 käytännöt ovat kyvykkyyksiä tehdä palvelunhallintaan liittyviä asioita käytännössä. Käytäntöjä on yhteensä 34, jotka jaetaan yleisiin-, palvelunhallinnan- ja teknisiin käytäntöihin eli kyvykkyyksiin. Yleisenä kyvykkyytenä voidaan mainita jatkuva parantaminen ja tietämyksenhallinta. Palvelunhallinnan kyvykkyyksiä ovat palvelupyyntöjen hallinta, heurähteiden hallinta, ongelman hallinta, muutoksenhallinta, jakelun hallinta, palvelun konfiguraation hallinta ja IT-omaisuuden hallinta. Teknistä kyvykkyyttä ovat käyttöönoton hallinta, infrastruktuurin ja alustojen hallinta sekä ohjelmistojen kehittäminen ja hallinta. (ITIL Foundation 2019, 76.) Aikaisemmasta poiketen palveluomaisuuden- ja konfiguraationhallinta on jaettu kahdeksi eri käytännöksi. Nyt molempien osalta palvelu- ja arvona-
kökulma nousee korostuneemmin esille.

3 PALVELUOMAISUUDEN- JA KONFIGURAATIONHALLINTA

Kuten aikaisemmin on todettu, niin ITIL 4 viitekehys ei kumoa eikä korvaa prosesseihin perustuvaa palvelun elinkaarimallia. Uusi viitekehys lähestyy palvelunhallintaa arvon näkökulmasta. Siksi seuraavissa kappaleissa kuvataan palveluomaisuuden- ja konfiguraationhallintaa huomioiden molemmat viitekehykset.

Palveluomaisuuden- ja konfiguraationhallinta (SACM, Service Asset Configuration Management) liittyy kaikkiin palvelun elinkaaren vaiheisiin ja se hallinnoi palveluomaisuutta ja konfiguraation rakenneosia (CI, Configuration Item) tukeakseen muita palvelunhallinnan prosesseja. Tavoitteena on muun muassa tuottaa ja ylläpitää määrämuotoista konfiguraatietietoa palveluomaisuudesta ja palveluiden tuottamiseen käytettävästä IT-infrastruktuurista koko sen elinkaaren ajan, varmistaa rakenneosien ja konfiguraatioiden eheys sekä tukea palvelujohtamista. (ITIL Perustason käsikirja 2013, 175-176.)

Palveluomaisuuden- ja konfiguraationhallinnan (SACM) kriittisistä menestystekijöistä voidaan mainita konfiguraation rakenneosat (CI), palvelunhallintaprosessien tuki ja konfiguraationhallintajärjestelmä (CMS, Configuration Management System). Konfiguraation rakenneosat tulee kirjata, hallita ja niiden eheys suojata koko palvelun elinkaaren ajan. Mahdollisimman tarkka ja reaaliaikainen konfiguraatietieto tukee palvelunhallintaprosesseja ja varmistaa osaltaan prosessien toiminnan ja vaikuttavuuden. Konfiguraatitiedon hallinta ja käytettävyys vaatii jätävästi ylläpidetyn konfiguraationhallintajärjestelmän. (ITIL Perustason käsikirja 2013, 182-183.)

ITIL 4 viitekehyksessä palveluomaisuudenhallinta ja konfiguraationhallinta on eriytetty omiksi käytännöiksi. IT-palveluomaisuuden hallinnan tarkoituksena on maksimoida omaisuuden arvo, hallita kustannuksia ja riskejä. Lisäksi tarkoituksena on tukea omaisuuden hankkimista, uudelleenkäyttöä ja hävittämistä koskevaa päätöksentekoa sekä täyttää lainsäädännölliset- ja sopimusvaatimukset. Yleensä organisaatioissa omaisuutta hallitaan vakiintuneiden käytäntöjen mukaisesti. Hallinnan onnistuminen vaatii omaisuuseristä tarkkoja tietoja, joita ylläpidetään omaisuusrekisterissä. Omaisuusinventointien lisäksi tiedon tulisi palvella myös muita kyvykkyyksiä. Siksi tiedot on hyvä tallentaa ja ylläpitää osana sellaisia prosesseja, joissa omaisuuden tilaa muutetaan. Esimerkkinä

mainittakoon uuden laitteen toimitus, käyttöönotto tai hävittäminen. Omaisuuden, kustannusten ja palvelujen arvo on hyvä ymmärtää taustalla vaikuttavana tekijänä. IT-omaisuuden hallinta tuo näkyväksi omaisuuden arvon, toimii avaintekijänä onnistuneelle palvelunhallinnalle ja on hyödyllinen muille käytännöille. (ITIL Foundation 2019, 124-125.)

ITIL 4:n mukaan konfiguraationhallinta käsittelee myös palveluita konfiguraation rakennesoina (CI). Konfiguraationhallinta auttaa organisaatiota ymmärtämään, kuinka monet rakennesoinat toimivat yhdessä ja osallistuvat palvelun tuottamiseen. Konfiguraatitietojen keräämiseen ja ylläpitoon tarvittava työ tulisi olla tasapainossa arvon kanssa, jonka tiedot luovat. Suuren tietomäärän kerääminen ja ylläpito voi olla organisaatiolle kallista suhteessa tietojen tuottamaan arvoon. Vaatimusten tulisi perustua ymmärrykseen organisaation tavoitteista ja siitä, kuinka konfiguraationhallinta edistää arvon luomista. Lisäksi on hyvä tiedostaa konfiguraationhallinnan luoma epäsuora arvo. Tämä epäsuora arvo mahdollistaa muiden käytäntöjen, kuten esimerkiksi muutoksenhallinnan tehokkaan toiminnan. (ITIL Foundation 2019, 140.)

3.1 Peruskäsitteet

Palveluomaisuudella tarkoitetaan mitä tahansa kyvykkyyttä tai resurssia, joka voi edistää palvelun tuottamista. Palveluomaisuutta ovat esimerkiksi ohjelmistolisenssi, tietoliikenneverkon reititin, kytkin tai yksittäisen työntekijän tietämys. (ITIL Perustason käsikirja 2013, 178.)

Konfiguraation rakennesoina (CI) on palveluomaisuuden osa ja samalla yksi palvelutuotannon yksilöitävä komponentti, jota pitää hallita palvelun toimittamiseksi. Yksittäistä tietoa konfiguraation rakennesoinasta kutsutaan attribuutiksi. Tietoliikenneverkon reitittimen ja kytkimen attribuutteja ovat esimerkiksi sarjanumero, nimi ja sijainti. (Bon van 2009, 115.) Rakennesoinien ominaisuus- ja yhteyskuvauksia nimitetään konfiguraatitietueiksi, joita säilytetään CMDB:n (Configuration Management Database) konfiguraatitietokannassa (ITIL Perustason käsikirja 2013, 178).

Linkkiä reitittimen ja kytkimen välillä kutsutaan relaatioksi. Tämä kuvaa miten kaksi rakennesoinaa toimivat yhdessä muodostaakseen palvelun joko keskenään tai yhdessä muiden rakennesoinien kanssa. Riippuvuuksien avulla on mahdollista luoda palvelujen, palveluomaisuuden ja infrastruktuurin looginen malli. (Bon van 2009, 115.)

Konfiguraation rakenne esittää suhteet ja hierarkian konfiguraation rakenneosien välillä. Rakenneosat muodostavat konfiguraation. Konfiguraation rakenneosien tietoja ylläpidetään ja niille tulee määrittää perustaso. Tämä mahdollistaa epäonnistuneen muutoksen, julkaisun tai laiterikon jälkeen paluun tunnettuun ja toimivaan perustason konfiguraatioon. (Bon van 2009, 115.)

3.2 Tiedonhallinta

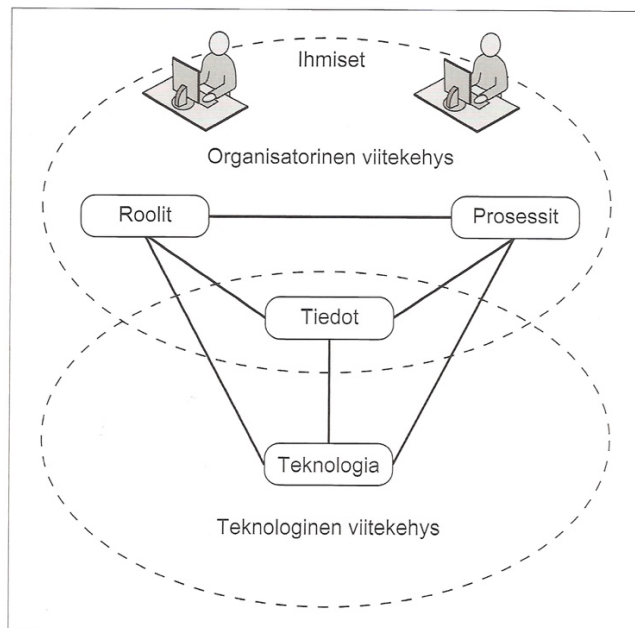
Tietoverkon palveluomaisuuden- ja konfiguraationhallintaan liittyy tiedon ja tietämyksen hallintaa. Tiedon määritelmä ja merkitys riippuu asiayhteydestä. Dokumentoiduksi tiedoksi kutsutaan tietoa, jota organisaatiolla on tarve hallita ja ylläpitää. Tieto voi olla missä tahansa tallennusmuodossa ja millä tahansa tietovälineellä ja mistä tahansa lähteestä peräisin. (SFS-ISO/IEC 20000-1:2018, 10.) Sydänmaanlakan (2012, 176) mukaan tiedon johtaminen on prosessi, jossa luodaan, hankitaan, varastoidaan, jaetaan ja sovelletaan tietoa. Tiedon hallinnassa korostuu teknologian merkitys. Ihmisen ja organisaation näkökulma painottaa tiedon ja osaamisen hallintaa sosiaalisen vuorovaikutuksen kautta. (Lönnqvist ym. 2007, 27.)

Tietämyksenhallinnasta käytetään usein termiä "knowledge management". Asiayhteydestä riippuen termiä käytetään myös tiedonhallinnasta ja tietojohdamisesta (Suurla 2001, 25). ITIL 3-viitekehyksessä tietämyksenhallinta kuvataan prosessina, joka sijoittuu palvelun elinkaarimallissa palvelutransitioon. Prosessin tarkoitus on jakaa näkökulmia, ideoita, kokemuksia ja informaatiota varmistaen, että nämä ovat saatavilla oikeassa paikassa oikeaan aikaan tietämykseen perustuvien päätösten tekemiseksi. Lisäksi prosessi parantaa tehokkuutta ilman, että tietämystä tarvitsee uudelleen etsiä. (ITIL Perustason käsikirja 2013, 205.) IT-palvelunhallinnan standardi käsittelee tietämystä palvelunhallintajärjestelmän (SMS) yhtenä tukitoimintona. Organisaation on määritettävä olennainen tietämys ja ylläpidettävä sitä. Tietämyksen tulee olla käytettävissä ja asianmukaisten henkilöiden saatavilla. (SFS-ISO/IEC 20000-1:2018, 23.)

ITIL korostaa palvelusuunnittelun neljän P:n tärkeyttä menestyvälle palveluntuotannolle. Jotta suunnitelmat ja käytännön tekeminen saadaan onnistumaan tarvitaan ihmisiä (engl. people), prosesseja (engl. processes), tuotteita (engl. products) ja kumppaneita (engl. partners). Tuotteita voivat olla palvelut, teknologiat ja työkalut. Kumppaneiksi luetaan muun muassa toimittajat, valmistajat ja myyjät. (Bon van 2009, 31.) Kuten aikai-

semmin on todettu, niin palveluomaisuuden- ja konfiguraationhallintaan liittyy myös tiedonhallintaa, jonka suunnittelussa edellä kuvatut neljä P:tä tulisi huomioida mahdollisimman hyvin.

Jyväskylän yliopiston monivuotisen tutkimustyön ja yritysten yhteistyön tuloksena kehitettiin tiedonhallinnan suunnittelun viitekehys nimeltään timanttimalli. Kuvan 7 timanttimallin organisatorisen ja teknologisen viitekehysten osia ovat roolit, prosessit, tiedot ja teknologiat. (Kaario & Peltola 2008, 136-137.)



Kuva 7. Tiedonhallinnan suunnittelun viitekehys (Kaario & Peltola 2008, 137).

Organisatorinen viitekehys pyrkii varmistamaan, että organisaation sosiaalinen ulottuvuus huomioidaan tiedonhallinnan suunnittelussa. Keskiössä ovat ihmiset, joilla prosessinäkökulman lisäksi on merkittävä tiedon käyttäjän ja ylläpitäjän roolinäkökulma tiedonhallintaan. Roolit voivat olla monen tyyppisiä ja eri tasoisia. (Kaario & Peltola 2008, 137.)

Teknologinen viitekehys käsittää tiedon hallintaan, taltiointiin ja edelleen välittämiseen liittyvän teknologian, esimerkiksi sovellukset ja laiteinfrastruktuurin. Tieto toimii kahden viitekehysten rajapinnalla tukien organisaation toimintaa. Teknologia mahdollistaa tiedon tehokkaan käsittelyn ja varastoinnin. Tiedonhallintasuunnitelmaa laadittaessa tulee huomioida organisatorisen ja teknologisen viitekehysten osien väliset suhteet painotuksineen. (Kaario & Peltola 2008, 138.)

Timanttimalia soveltaen tietoliikenneverkon verkkolaitteiden konfiguraationhallinnan osat voidaan tunnistaa seuraavasti: Teknologiaa edustaa tietoliikenneverkon kytkimet ja reitittimet, joista verkkolaitteiden hallinta- ja valvontajärjestelmä automaattisesti kerää ja myös ylläpitää tietoa reaaliajassa. Tiedon määrä on valtava suhteessa tarpeeseen. Tiedointegraation kautta vain tarvittava ja erikseen määritelty tieto siirretään ja tallennetaan konfiguraatietietokantaan (CMDB, Configuration Management Database). Tiedon käyttäjien rooleissa voivat olla suunnittelijat, tieto- ja tietoliikenneverkkojen tuotantovastavat, verkon valvonta ja hallinta, kybertoimiala, kenttätoiminta, palvelunhallinta, materiaalihallinto, taloushallinto sekä laitetoimittajat ja kumppanit. Prosessinäkökulman painotus voidaan kohdistaa esimerkiksi konfiguraationhallintaan, häiriönhallintaan, muutoksenhallintaan ja ongelmanhallintaan sekä palvelupyyntöprosessiin. Kuvan 6 perusteella haasteeksi saattaa muodostua kaikkien osien yhteensovittaminen timanttimalin eri rajapinnoissa.

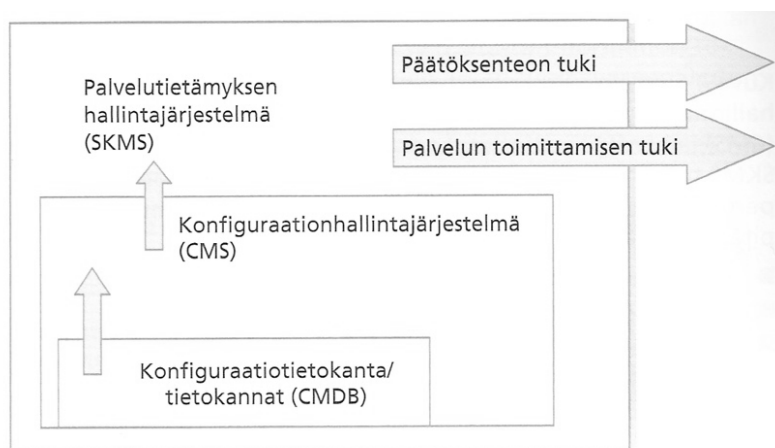
3.3 Palvelutietämyksen hallintajärjestelmä

IT-alan palveluomaisuuden- ja konfiguraationhallinta sisältää samankaltaisia piirteitä kuin kappaletavaraa valmistavan yrityksen tuotetiedon hallinta tai yksittäisen projektin konfiguraationhallinta. Näissäkin tapauksissa konfiguraationhallinta on tiedon hallintaa, joka pääsääntöisesti vaatii tuekseen tietojärjestelmään nojaavan hallintajärjestelmän. Yrityksen tarpeista ja kypsyydestä riippuen tietojärjestelmien käyttö voidaan rajata koskemaan vain tiettyjä osa-alueita tai prosesseja. (Sääksvuori & Immonen 2002, 20.)

ITIL:n mukaan tietämyksenhallinnan yksi tavoitteista on ylläpitää palvelutietämyksen hallintajärjestelmää (SKMS, Service Knowledge Management System). Kuva 8 havainnollistaa palvelutietämyksen hallintajärjestelmän pelkistettyä rakennetta. Järjestelmä muodostuu osista ja niiden välisistä suhteista. Järjestelmä sisältää konfiguraationhallintajär-

jestelmän (CMS, Configuration Management System) ja konfiguraationhallintatietokannan (CMDB, Configuration Management) sekä muita tietokantoja ja tietojärjestelmiä. Konfiguraationhallintajärjestelmä on joukko työkaluja, tietoa ja informaatiota.

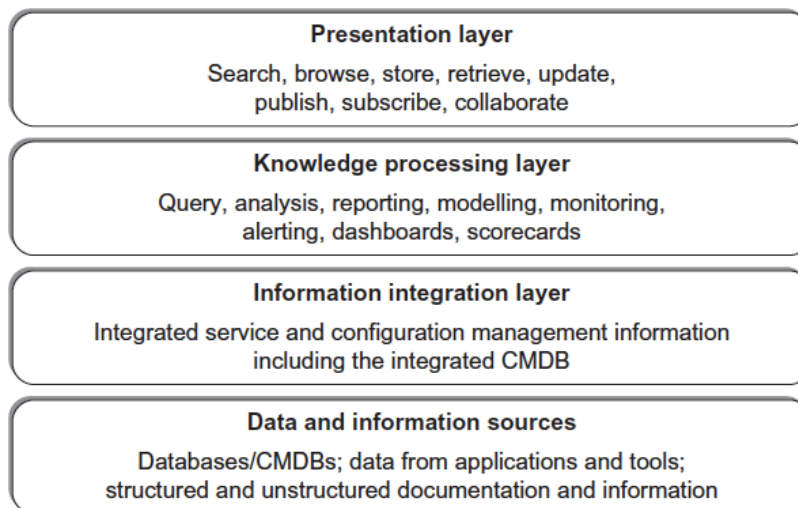
Konfiguraatietietokantaan tallennetaan konfiguraation rakenneosien (CI) tiedot koko elinkaaren ajan. (ITIL Perustason käsikirja 2013, 205, 207-208.) Tiedon lähteistä riippuen konfiguraationhallintajärjestelmästä käytetään myös nimeä CMDB-järjestelmä.



Kuva 8. Palvelutietämyksen hallintajärjestelmä (ITIL Perustason käsikirja 2013, 208).

Tiedon määrä ja sisältö luonnollisesti rikastuu tultaessa järjestelmän ytimestä sen ulkokehälle. Myös tiedon tallennusformaatti ja esitystapa saattaa vaihdella riippuen missä osassa järjestelmää mitään tietoa säilytetään ja käytetään. Järjestelmässä olevan tiedon käyttötarve riippuu prosessista, roolista tai käyttäjäryhmästä.

Konfiguraationhallintajärjestelmä (CMS) jaetaan kuvan 9 mukaan arkkitehtonisesti eri tasoihin. Tasoja ovat esitystaso (engl. presentation layer), tietämyksen käsittelytaso (engl. knowledge processing layer) ja tietojen integrointitaso (engl. information integration layer). Alimmalla tasolla on tieto- ja informaatiolähteet sekä työkalut (engl. data and information source).



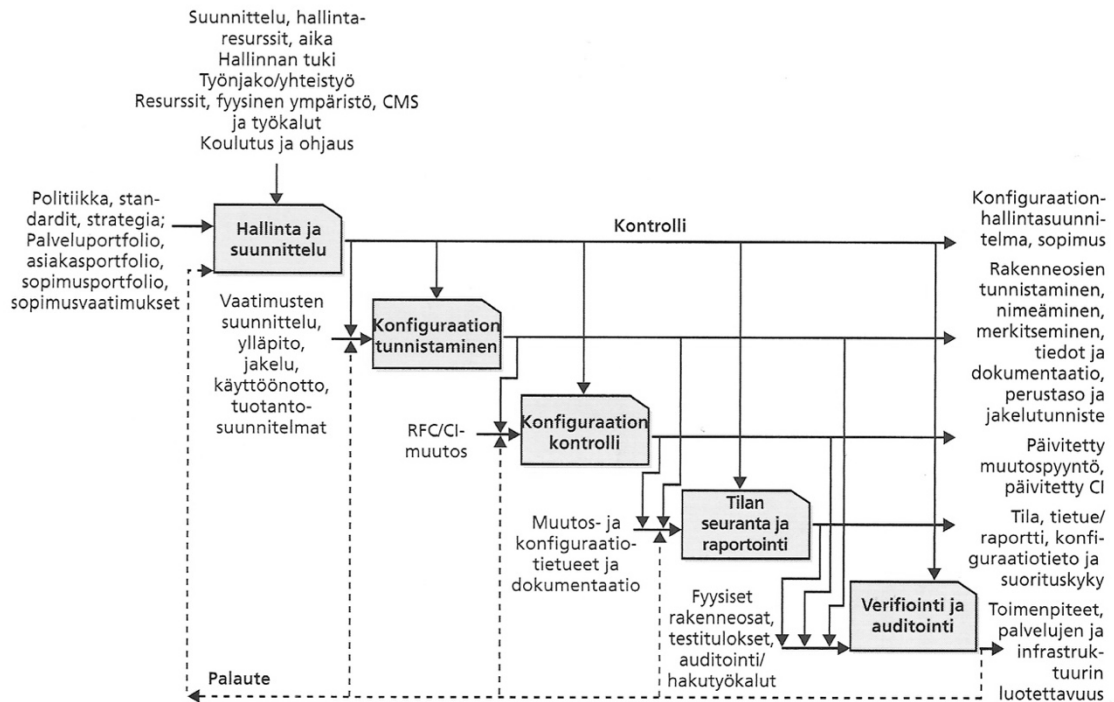
Kuva 9. Konfiguraationhallintajärjestelmän tasot (Shirley & Norfolk 2014, 4).

Esitystaso (engl. Presentation layer) mahdollistaa käyttäjälle tiedon etsimisen, selaamisen, päivittämisen ja julkaisun. Tietämyksen käsittelytason (engl. Knowledge processing layer) työkaluilla tuotetaan analyyskejä, raportoidaan, kerätään hälytystietoja ja suoritetaan kapasiteetin hallintaa. Tietämyksen käsittelytaso kerää tiedot siirrettäväksi esitystasolle. Tietojen integrointitasolla (engl. Information integration layer) sijaitsee muun muassa yhdistelmä CMDB-tietokantoja ja metatietoja. Yhdistetty CMDB mahdollistaa sovellustietojen integroinnin infrastruktuuritietoihin luoden samalla kootut konfiguraatitiedot koko palvelusta. Integraatitason tietoja voidaan käyttää esitys- ja tietojenkäsittelykerroksella. Tasolla tieto- ja informaatiolähteet sekä työkalut (engl. Data and information sources) sijaitsee varsinaiset tietolähteet sekä konfiguraationhallinnan, inventoinnin ja auditoinnin työkalut sovellustietoineen. Tämä taso tarjoaa alustan erillisille CMDB-tietokannoille, mediakirjastoille, ohjelmistolisenssien dokumentaatiolle ja muille dokumenteille. (Shirley & Norfolk 2014, 4, 10-11.)

Johtavat CMS- ja CMDB-ratkaisut on rakennettu tukemaan keskitettyä lähestymistapaa CMS-järjestelmään. Tämä ei tarkoita sitä, että kaikki tieto on fyysisesti samassa tietokannassa. Lähtökohtaisesti perustiedot pyritään tallentamaan CMDB-kantoihin, joista on linkitykset muihin tietovarastoihin ja niiden sisältöön. Järjestelmän arvoa organisaatiossa voidaan lisätä linkittämällä järjestelmään muita avaintoimintoja, kuten esimerkiksi analytiikkaa, palveluomaisuuden hallintaa ja työnohjausjärjestelmä. (BMC Software 2016, 3.) Tiedon ja tietoverkkojen eri suojaustasot saattavat rajoittaa linkityksiä järjestelmän eri tietovarastojen välillä.

3.4 Palveluomaisuuden- ja konfiguraationhallintaprosessin aktiviteetit

Palveluomaisuuden- ja konfiguraationhallintaprosessin (SACM) aktiviteetteja ovat hallinta ja suunnittelu, konfiguraation tunnistaminen, konfiguraation valvonta, tilan seuranta ja raportointi sekä verifiointi ja auditointi (Bon van 2009, 114). Aktiviteetteja sekä niihin kohdistuvia syötteitä ja tuotoksia esittää kuva 10.



Kuva 10. Palveluomaisuuden- ja konfiguraationhallinta (Bon van 2009, 114).

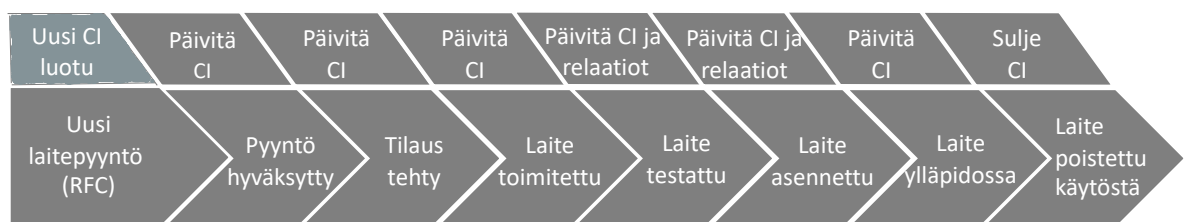
Hallinta- ja suunnitteluaktiviteetin tulee määrittellä konfiguraatiohallinnan taso ja kuinka tämä taso voidaan saavuttaa. Konfiguraation tunnistamisen osassa määritetään muun muassa tarpeelliset konfiguraation rakenneosat, niiden nimeämissä käytännöt, tunnisteet, keskinäiset suhteet ja rakenneosien oleelliset attribuutit. Kontrolli varmistaa ettei rakenneosaa muuteta, vaihdeta tai poisteta ilman sovittua toimintatapaa. Tilan seuranta ja raportointi kattaa rakenneosan koko elinkaaren. Tilatietoja voivat olla esimerkiksi kehityksessä, käytössä tai poistettu. Verifiointi ja auditointi varmistaa, että konfiguraation rakenneosien dokumentoitu tieto on ajantasaista ja vastaa todellista tilannetta. (Bon van 2009, 117-118.)

Onnistunut ja rationaalinen palveluomaisuuden -ja konfiguraationhallinnan toteuttaminen arjessa on helpommin sanottu kuin tehty. Käytännön tekemisen taustalla tulisi olla

suunnitelma tai erikseen määritetystä osasta suppeampi toimintamallin kuvaus. Kuvan 10 esimerkki aktiviteeteista syötteineen ja tuotoksineen antaa suuntaviivoja suunnitelman laatimiseen tai toimintamallin kuvaamiseen. On hyvä miettiä tapauskohtaisesti mikä on suunnitelman dokumentoitu muoto ja kuinka laajalle ja yksityiskohtaiselle suunnitelmalle on tarvetta.

3.5 Konfiguraation rakenneosan elinkaarenhallinta

Konfiguraation rakenneosan (CI) elinkaarenhallinnan lähtökohtana on tunnistettu ja dokumentoitu rakenneosa tai rakenneosaryhmä. Yksittäisen ryhmän alaisuuteen voi kuulua monia samankaltaisia rakenneosatyyppisiä, kuten esimerkiksi kannettavia työasemia, tulostimia tai muita vastaavia päätelaitteita. Kullakin laitteella voi olla erilaisia ominaisuuksia eli attribuutteja ja ne voivat suorittaa erilaisia toimintoja. Laitteita yhdistää kuitenkin samat elinkaaren vaiheet. Kuva 11 havainnollistaa kuinka laitteen konfiguraation rakenneosan attribuuttitietojen päivitys on kytketty laitteen elinkaaren vaiheisiin. (BMC Software 2016, 148-149.)



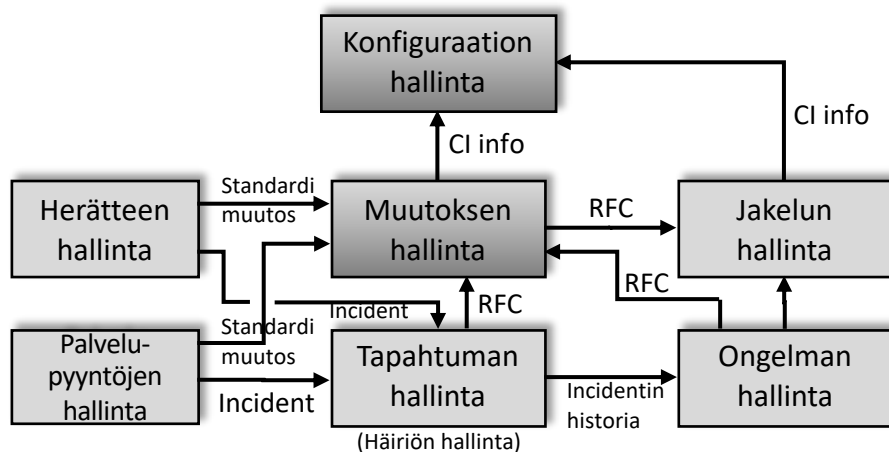
Kuva 11. Konfiguraation rakenneosan elinkaarenhallinta (mukaillen BMC Software 2016, 150).

Uusi konfiguraation rakenneosa (CI) voidaan luoda konfiguraationhallintatietokantaan (CMDB) joko ennen uuden laitepyynnön hyväksymistä tai sen jälkeen. Olennaista on sopia selkeä toimintatapa. Samalla määritellään kenen vastuulla on rakenneosan luominen, mitä laitetta pyyntö koskee ja milloin laitetta tarvitaan. Pyyntön hyväksymisvaihe kertoo, kuka pyynnön käsittelee ja mikä on käsittelyajankohta. Lisäksi varmistetaan rahoituksen kohdennukset ja mahdolliset ehdot esimerkiksi laitteen omistusoikeudesta. Viimeistään tilausvaiheen käytettävissä oleva tieto hyödynnetään konfiguraation rakenneosatiedon päivittämiseen. Tällaisia tietoja ovat muun muassa valmistaja, merkki, malli ja tekniset ominaisuudet. Laitetoimituksen yhteydessä verrataan tilausta toimituksen

kanssa. Tässä vaiheessa voidaan dokumentoida toimituspäivä, sarjanumero ja täydentää muita puuttuvia teknisiä tietoja. Elinkaaren testausvaiheessa lisätään tieto omistajasta ja relaatioista. Ennen testausvaiheen päättymistä tulee varmistaa dokumentoidun konfiguraatitiedon tarkkuus ja riittävyys. Kaikki edellä tehty huolellinen tietojen keräys- ja dokumentointityö helpottaa asennusvaihetta merkittävästi. Asennuksen yhteydessä kirjataan asennuspäivämäärä, päivitetään relaatiotiedot ja luovutetaan laite tuotantokäyttöön. Ylläpitovaihetta varten määritellään attribuutit, joiden muutoksia seurataan ja päivitetään. Paras tapa on ohjata kaikki tilamuutokset muutoksenhallintaprosessin käsiteltäväksi. Laitteen käytöstä poistosta kirjataan päivämäärä ja poiston hyväksyjä. Tämän jälkeen rakenneos (CI) voidaan poistaa konfiguraationhallintatietokannasta. (BMC Software 2016, 150.)

3.6 Rajapinnat prosessien välillä

Palveluomaisuuden- ja konfiguraationhallinta tukee ja on yhteydessä kaikkien muiden palvelunhallinnan prosessien kanssa. Kääntäen voidaan todeta, että vahvat tukiprosessit ovat välttämättömiä CMDB-tietojen reaaliaikaisen päivittämisen ja oikeellisuuden varmistamisessa. Keskeisiä tukiprosesseja ovat tapahtumanhallinta (engl. incident management), ongelmanhallinta (engl. problem management) ja muutoksenhallinta (engl. change management). IT-organisaatioissa juuri näiden prosessien kypsyys on yleensä hyvällä tasolla. (Shirley & Norfolk 2014, 43.) Erityinen huomio tulee kiinnittää muutoksenhallintaan. Kokeneet asiantuntijat eivät suosittele CMDB-tietokannan käyttöönottoa ja käyttöä ellei muutoksenhallinta toimi (BMC Software 2016, 157). Kuva 12 on ote erään yrityksen laajemmasta suunnitelmakuvasta. Se laadittiin kartoitettaessa prosessi- ja sidosryhmärajapintoja CMDB-tietokannan käyttöönottoon liittyen. Kuva havainnollistaa konfiguraationhallinnan asemaa ja rajapintoja suhteessa muutoksenhallintaan ja muihin prosesseihin. (Drogseth ym. 2015, 40.)



Kuva 12. Erään yrityksen prosessirajapintoja (mukaillen Drogseth ym. 2015, 40).

Palvelupyyntöjen hallinta

Palvelupyyntöprosessi vastaa käyttäjien palvelupyyntöjen hallinnasta niiden elinkaaren ajan. On hyvä tiedostaa ettei tapahtumanhallinnan prosessinimeä käytetä vuonna 2011 päivitetysssä ITIL-julkaisussa. Tapahtumanhallinnan tehtävät ja toiminnallisuudet on jaettu palvelupyyntöprosessiin (engl. request fulfilment) ja häiriönhallintaprosessiin (engl. incident management). Jako on perusteltu, koska häiriö on pääsääntöisesti suunnittelemaan tapahtuma. Palvelupyyntö voi olla asiakkaan kysely, uuden työaseman asennus, kytkimen portin avaus tai suunnittelua vaativa tapahtuma. Palvelupyyntöön liittyvät mahdolliset muutokset on päivitettävä konfiguraationhallintajärjestelmään. Kaikki työnohjaus- ja tiketointityökalut eivät välttämättä tue edellä kuvattua jakoa. Työkalut tai jokin muu perusteltu syy saattaa ohjata organisaation käsittelemään sekä häiriöt että palvelupyyntöjä edelleen tapahtumanhallintaprosessissa. (ITIL Perustason käsikirja 2013, 253-254, 258.)

Herätteenhallinta

Herätteidenhallintaa käytetään tuotannon monitoroinnin ja hallinnan perustana. Tarkoituksena on koordinoita herätteiden havaitsemista, tulkintaa ja päätöksentekoa toteutettavista hallintatoimenpiteistä. Herätteidenhallinnan tavoitteena on havaita mahdollisimman automatisoidusti tilamuutoksia, joilla on merkitystä konfiguraation rakenneosan (CI) tai IT-palvelun hallinnan kannalta. Palveluomaisuuden- ja konfiguraationhallinta käyttää

herätteitä määrittämään rakenneosien nykytilan. Herätteet ovat myös käynnistävä tekijä monille muille prosesseille ja palvelunhallinnan toimenpiteille. Lisäksi herätteidenhallinta tuottaa tilannekuvaa ja vertailutietoa tuotannon suorituskyvystä suhteessa esimerkiksi palvelutasosopimuksiin. (ITIL Perustason käsikirja 2013, 244-245, 250.)

Häiriönhallinta

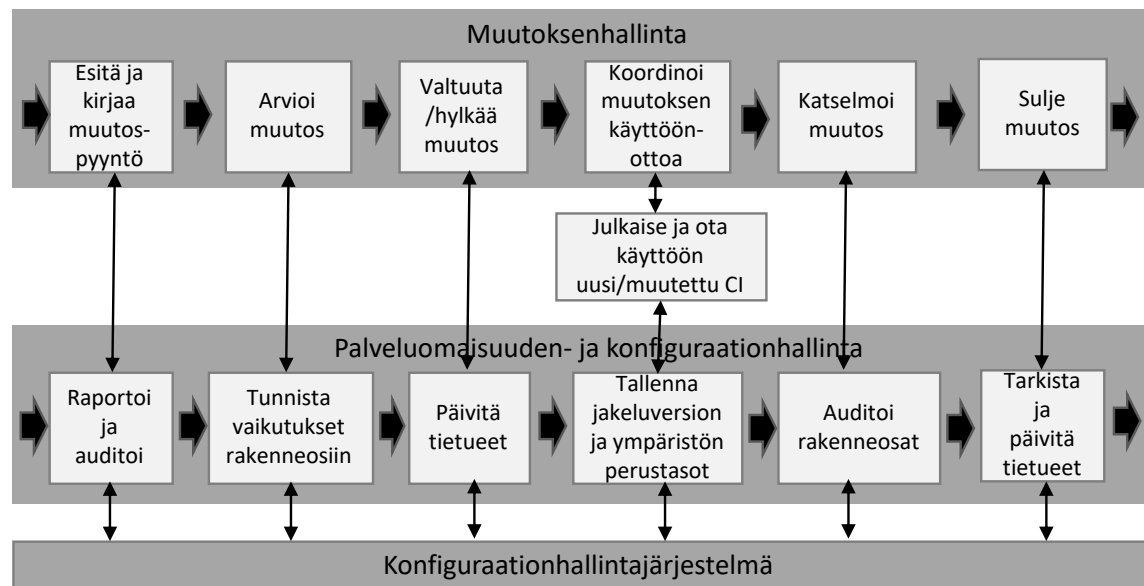
Häiriönhallinta vastaa kaikkien häiriöiden käsittelystä ja niiden elinkaaren hallinnasta. Häiriönhallinta varmistaa palvelun mahdollisimman nopean palauttamisen ja minimoi vaikutukset liiketoimintaan. Palveluomaisuuden- ja konfiguraationhallinnan avulla tunnistetaan häiriöitä, helpotetaan viallisten laitteiden havaitsemista ja häiriön vaikutusten arviointia. Häiriöt voivat olla loppukäyttäjän, teknisen henkilöstön ja tietoverkon valvontatyökalun havaitsemia vikoja tai muita herätteitä. Tietoverkon aktiivilaitteen konfigurointivirhe voidaan tulkita häiriöksi, vaikka se ei ole vaikuttanut palveluun. Palvelutoiminnan normaalitilassa palvelut ja konfiguraation rakenneosat toimivat sovitulla tasolla. (ITIL Perustason käsikirja 2013, 219-220, 227.)

Ongelmanhallinta

Ongelmanhallinta vastaa ongelmien hallinnasta koko elinkaaren ajan. Se pyrkii ennakkoivasti estämään häiriöiden ja ongelmien kielteiset vaikutukset liiketoimintaan. Ennakkoivalla toiminnalla pyritään tukemaan palvelun parannuskohteiden havaitsemista ja käyttöönottoa. Lisäksi ongelmanhallintaan kuuluu toistuvien häiriöiden juurisyyyn selvittäminen ja ratkaisun määrittäminen. Konfiguraationhallintajärjestelmä avustaa ongelmanhallintaa tunnistamaan viallisen rakenneosan (CI) sekä tukee ongelmien ja ratkaisujen vaikutusten määrittelyä. Ongelmanhallinnan tehtävänä on varmistaa, että ratkaisut toteutetaan oikeita menettelytapoja käyttäen. Esimerkiksi pyyntö tietoverkon kapasiteetin lisäyksestä tulee osoittaa muutoksenhallintaan. Ongelmanhallinnan elinkaaren vaiheita ovat havaitseminen, tutkiminen, dokumentointi, ratkaiseminen ja sulkeminen. (ITIL Perustason käsikirja 2013, 231-232, 240.)

Muutoksenhallinta

Muutoksenhallinta vastaa kaikkien muutosten hallinnasta ja koordinoinnista koko elinkaaren ajan. Se mahdollistaa hyödyllisten muutosten tekemisen minimoiden samalla palveluille aiheutuvia häiriöitä. Muutoksenhallinta käsittelee fyysiseen, virtuaaliseen tai muuhun palveluomaisuuteen kohdistuvat konfiguraation rakenneosien (CI) muutokset. Palveluomaisuuden- ja konfiguraationhallinta tuottaa päivitettyä konfiguraatietietoa muutosten suunnittelun, arvioinnin ja toteutuksen tueksi. Muutoksenhallinnan elinkaaren vaiheita ovat kirjaus, arviointi, priorisointi, suunnittelu, testaus, toteutus, dokumentointi, katselmointi ja sulkeminen. (ITIL Perustason käsikirja 2013, 163-164, 172.) Kuvan 13 työnkulkukaavio kuvaa yhteistoimintarajapintaa muutoksenhallinnan sekä palveluomaisuuden- ja konfiguraationhallinnan välillä.



Kuva 13. Muutoksenhallinnan sekä palveluomaisuuden- ja konfiguraationhallinnan välinen rajapinta (mukaillen ITIL Service Strategy 2011, 87).

Muutosten laajuus ja vaikuttavuus palveluihin vaihtelee. Usein toistuvat pienet muutokset voidaan toteuttaa standardimuutoksina. Niiden toteuttamiselle on ennalta hyväksytty valtuutus tai muutoksenhallintapäällikön hyväksyntä. Laajat ja merkittävän riskin muutoksista laaditaan muutospyyntö (RFC, Requests for Change), jonka hyväksyy erikseen nimetty muutoskomitea (CAB, Change Advisor Board) tai yrityksen johto. Muutoksiin liittyviä peruskysymyksiä ovat: Kuka pyysi muutoksen?, mikä on muutoksen syy?, mikä on muutoksen toivottu tulos?, mitä riskejä muutoksen tekemiseen liittyy?, mitä resursseja

muutoksen toteuttamiseen tarvitaan?, kuka vastaa muutoksen rakentamisesta, testauksesta ja toteuttamisesta? sekä mikä on tämän muutoksen ja muiden muutosten välinen suhde?. (Drogseth ym. 2015, 36.)

Jakelun- ja käyttöönoton hallinta

Jakeluversioiden suunnittelu, ajoitus ja valvonta ovat jakelun- ja käyttöönotonhallinnan vastuulla. Se tuottaa päivityksiä konfiguraationhallintajärjestelmään (CMS), mutta on myös itse riippuvainen järjestelmässä olevista tiedoista. Jakelun- ja käyttöönotonhallinnan tavoitteena on muun muassa luoda ja testata mediakirjastoissa säilytettävät jakelupaketit sekä suojata jakelun yhteydessä olemassa olevien palvelujen eheys. Lisäksi se varmistaa, että organisaation ja sidosryhmien muutoksia hallitaan sekä tietämys siirretään IT-organisaatiolle, asiakkaille ja käyttäjille. (ITIL Perustason käsikirja 2013, 184-185, 190.)

4 TEEMAHAASTATTELUN TOTEUTUS JA TULOKSET

Opinnäytetyön tutkimusotteena käytettiin kvalitatiivista menetelmää. Aineisto hankittiin teemahaastatteluilla. Kaikki haastattelut nauhoitettiin, jonka jälkeen aineisto litteroitiin teema-alueiden mukaisesti. Teemahaastattelun purkuun ja analysointiin käytettiin osaltaan diskurssianalyysin menetelmää. Tulosten esittämisen perusteina on litteroitu ja analysoitu aineisto. (Hirsjärvi ym. 2015, 222-226.)

Pääesikunnan myöntämän tutkimusluvan mukaan osallistuminen tutkimukseen tulee olla vapaaehtoista, eikä siihen osallistuneita henkilöitä saa olla tunnistettavasti esillä tutkimusraportissa (Pääesikunta 2017 ja 2019). Tutkimusluvan lupaehtoja on noudatettu teemahaastattelujen toteutuksessa, aineiston analyysissä ja tulosten esittämisessä.

4.1 Teemahaastattelun osallistujat ja haastattelujen toteutus

Teemahaastatteluun valittiin asiantuntijoita, joilla oli kokemusta tietoverkkojen suunnittelun eri tehtävistä, verkon valvonnasta ja hallinnasta sekä asentajan tehtävistä. Lisäksi haastatteluun valittiin asiantuntijoita, joilla oli prosessiosaamista, kokemusta palvelunhallintajärjestelmän ylläpidosta ja tuesta sekä kybertoimialalta.

Yksilö- ja tiimihaastattelut toteutettiin kesä-syyskuussa 2019 joko henkilökohtaisena tapaamisena tai verkkokokous-sovellusta hyödyntäen. Kymmeneen eri haastattelutapahtumaan osallistui yhteensä viisitoista henkilöä. Kaikilla haastatteluun osallistuneilla henkilöillä on laaja-alainen sekä usean vuoden tai vuosikymmenien mittainen kokemus IT-alan tehtävistä.

Teemahaastattelun kysymysrunko oli kaikille haastateltaville sama. Kysymykset lähetettiin sähköpostilla haastattelukutsun yhteydessä. Tutkimusilmiö, tutkimuksen tarkoitus ja tavoitteet esiteltiin haastateltaville ennen haastattelua. Haastatteluissa käsiteltiin tietoverkon verkkolaitteiden konfiguraationhallintaa kokonaisuutena, mutta kohdentuen tarkemmin verkon kytkimiin ja reitittäjiin. Aineiston litterointi osoitti haastatteluissa kertyneen tietomäärän liian laajaksi opinnäytetyön tarkoitukseen ja tarkentuneisiin tavoitteisiin nähden. Litterointivaiheen jälkeen aineisto rajattiin koskemaan neljää eri teemaa, joiden perusteella aineisto analysoidaan ja tulokset esitetään. Rajauksessa huomioitiin myös kertyneen tiedon tietoturvaluokan asettamat rajoitteet julkisessa raportissa.

Teemahaastattelun kysymysrunko on esitetty liitteessä 1. Haastattelun teemoja olivat

- konfiguraation tunnistaminen
- konfiguraation kontrolli
- tilan seuranta ja raportointi
- prosessit ja roolit.

4.2 Konfiguraation tunnistamisen tulosten käsittely

Konfiguraation tunnistamisessa määritetään tarpeelliset konfiguraation rakenneosat, niiden nimeämiskäytännöt, tunnistet, keskinäiset suhteet ja rakenneosien oleelliset attribuutit (Bon van 2009, 117).

Kaikki haastateltavat kokivat, ettei organisaatiossa välttämättä tunneta konfiguraation peruskäsitteitä teoreettisen määrittelyn näkökulmasta. Käsitteet ovat osiltaan tuttuja ITIL-kurssin käyneiden joukossa ja niiden sisältöä sovelletaan konfiguraationhallinnan käytännön tekemisessä. Käsitteiden merkityksen ymmärtämiseen vaikuttaa myös käytetty kieli. Esimerkiksi käsite konfiguraation rakenneosa (CI, Configuration Item) saattaa kertoa asiasta enemmän englannin kielellä ilmaistuna kuin saman asian ilmaiseminen suomeksi. Käsitetason osaaminen koetaan asiantuntijuudeksi, jota esimerkiksi kentällä työskentelevät asentajat eivät tarvitse tai siitä ei ole hyötyä.

Haastateltavilla ei ole selkeää kokonaiskuvaa verkkolaitteiden konfiguraation tunnistamisen toimintatavasta. Tunnistamista tehdään päivittäin mutta tekemisen tapa ja siitä saatavaa tietoa käytetään lähinnä oman työtehtävän tarpeita varten. Tästä seuraa, että konfiguraatiotieto sirpaloituu eikä palvelutuotannon prosessit kykene hyödyntämään tietoja tehokkaasti. Useamman haastateltavan mukaan olennaista ei ole yksittäinen tieto vaan kokonaisuus, josta selviää verkon rakenne ja verkkolaitteiden väliset suhteet eli relaatiot. Tieto kokonaisuudesta ja riittävä osaaminen tukevat palvelun palauttamista viikatilanteissa.

Teknisen konfiguraatiotiedon tunnistaminen, keräys ja ylläpito kohdistuu verkkolaitteiden sähköiseen konfiguraatioon ja itse fyysiseen laitteeseen eli "rautaan". Konfiguraatioiden perustasot tunnistetaan, ne on dokumentoitu ja tarvitsijoiden saatavilla. Haastateltavat käyttivät perustasosta myös nimeä mallikonfiguraatio. Edellä kuvattua työtä tehdään manuaalisesti ja verkon hallintajärjestelmillä automaattisesti. Monesti hallintajärjestelmät

ovat laitevalmistajien omia ylläpitotyökaluja. Lisäksi tukena käytetään erilaisia verkko-suunnitelmia- ja kuvia sekä laitetoimittajien ilmoittamia laitetietoja. Taulukoon 2 on listattu haastatteluissa esille nousseita tietoverkkoon tai verkkolaitteisiin liittyviä konfiguraation rakenneosien (CI) attribuutteja, joita tarvitaan suunnittelu- ja ylläpitotyöhön laitteiden elinkaaren eri vaiheissa.

Taulukko 2. Tietoverkon tai laitteen konfiguraation rakenneosan (CI) attribuutteja.

Tietoverkon tai laitteen konfiguraation rakenneosan (CI) attribuutteja		
Valmistaja	Porttikapasiteetti	Konfiguraation historiatieto
Laitetyyppi	Korttikalustus	Relaatiot
Laitemalli	Käytettävä protokolla	Tunnistetut palvelun käyttäjät
Sarjanumero	Mitkä palvelut reitittimessä on päällä	Verkon suojaustaso/tietoturvaluokka
Ohjelmistoversio, esim. IOS (Internetwork Operation System)	Reitittimen ID-arvot (Router ID)	Konfiguraation perustaso (Mallikonfiguraatio)
Sijainti, Location (SNMP, Simple Network Management Protocol)	WAN linkkiosoite (Wide Area Network)	Dokumentit (Verkon loogiset kuvat)
IP-osoitteet CIDR muodossa (Classless Inter-Domain Routing)	Rungon väliverkon osoite	Virransyötön kapasiteetti ja toteutus laitteelle (esim. PoE, Power over Ethernet)
VLAN-tiedot (Virtual Location Area Network)	Loopback osoite/Ohjelmistointerface	Laitteen käynnissäoloaika (Uptimes)
Laitteen nimi (Hostname)	Liityntä ja kuvaukset (Description)	Laitemallin myynnin päättymispäivä (End-of-Sale Date)
Ylläpitovastuullinen		Laitemallin tuen päättymispäivä (End-of-Support Date)

Suunnittelun sekä verkon valvonnan ja hallinnan toimijoilla konfiguraatietiedon tarve on pääosin samanlainen mutta laajempi kuin muilla haastateltavilla. Tiedon tarve liittyy suunnitteluun, laitteiden elinkaaren hallintaan ja verkko-operointiin. Kybertoimijan tietotarve on osiltaan yhtenevä edellä mainittujen kanssa. Kybertoimija hyödyntää tietoja tietoturvaohjeiden ennakoiwaan tunnistamiseen, reaaliaikaiseen reagointiin ja verkkojen sekä palveluiden suojaamiseen. Kenttätoiminnan asentajalla ei ole jatkuvaa tarvetta rakenneosan yksityiskohtaiselle tiedolle. Pääsääntöisesti heille riittää, että työnohjausjärjestelmän työmääräykseen on kirjattu työn tekemisen edellyttämä tarpeellinen tieto. CMDB-työkalun ylläpitäjä mahdollistaa halutun tiedon viennin konfiguraationhallintatietokantaan joko manuaalisesti tai automaattisesti. Kaikkien kannalta tärkeää on osata hyödyntää saatavilla olevaa tietoa. Haasteeksi koettiin tiedonsaannin nopeus ja ajantasaisuus eri tilanteissa.

Suunnittelijoiden mukaan konfiguraation rakenneosien (CI) relaatioiden tunnistamista pidetään erityisesti korkeamman suojaustason verkoissa tietoturvaan liittyvänä vaatimuk-

sena. Automaattista tunnistamista ja erilaisia rajapintojen näkyvyyttä voidaan verkkokohdaisesti tai verkkolaitteiden välillä tarpeen mukaan teknisesti rajoittaa. Relaatioiden tunnistaminen voidaan nähdä myös verkon teknisen rakenteen mallintamisena. Eri valmistajien hallintatyökalujen ominaisuudet mahdollistavat liikennöivien verkkolaitteiden välisten relaatioiden piirtämisen automaattisesti. Työkalut eivät tunnista palveluita, vaan relaatio palvelun ja teknisen rakenteen välille pitää tehdä manuaalisesti.

Verkon hallintajärjestelmä kerää tietoverkosta valtavan määrän konfiguraatietietoa automaattisesti. Tietoa voidaan etsiä suoraan järjestelmästä tai siirtää muille medioille, kuten esimerkiksi konfiguraationhallintatietokantaan. Tiedon hyödyntäminen suoraan hallintajärjestelmästä edellyttää muun muassa käyttöoikeuksia järjestelmään ja laajempaa osaamista. Toisaalta yhteiskäyttöinen konfiguraationhallintatietokanta mahdollistaa tiedon laajemman hyödyntämisen ja käytön ICT-palvelutuotannon eri tarpeisiin. Kaikkien haastateltavien mukaan konfiguraatietietokanta on lähes tarpeeton ellei kannassa oleva tieto ole ajantasaista. Automaattinen tietojen siirto hallintajärjestelmän ja tietokannan välillä on rationaalisin tapa varmistaa tietojen ajantasaisuus. Manuaalinen toteutustapa on mahdollista mutta vaatii enemmän resursseja ja luo viiveitä kannassa olevan tiedon päivittämiseksi. Olennaisinta on määritellä kuka tietoa käyttää, mitä tietoa halutaan ja miten tieto kyetään ylläpitämään. Eräs haastateltavista linjasi asian seuraavasti: *”Periaate on se, että jokainen rakenneos ja attribuutti maksaa, jos ei suoraan rahaa, niin ainakin se kuluttaa resurssia”*. Konfiguraatietietokannan tarpeellisuutta voidaan perustella muun muassa eri toimijoiden yhteisillä tietotarpeilla sekä työnohjausjärjestelmän tiketöinnin ja raportoinnin kehittämällä.

4.3 Konfiguraation kontrollin tulosten käsittely

Konfiguraation kontrolli varmistaa ettei rakenneosaa lisätä, muuteta, vaihdeta tai poisteta ilman sovittua toimintatapaa (Bon van 2009, 118). Kontrollin varmistamisen tärkeänä tekijänä pidetään toimivaa muutoksenhallintaa. Esimerkiksi CMDB-tietokannan käyttöönottoa ja käyttöä ei suositella ellei muutoksenhallinta toimi (BMC Software 2016, 157).

Haastateltavat olivat yksimielisiä muutoksenhallinnan tärkeydestä. Muutoksenhallinnan periaatteita noudatetaan asiantuntijalähtöisesti siten, että jokainen verkkolaitteiden elinkaaresta vastaava toimija huolehtii omasta osuudestaan. Konfiguraatietiedon ylläpito-vastuu noudattaa pääosin samaa toimintamallia. Yhdistävänä tekijänä toimii organisa-

tion mukaiset johtosuhteet, toimialaohjaus vastuineen, verkon hallintajärjestelmä, muutosten tiketöintiin käytettävä työnohjaustyökalu ja jatkuva kommunikointi eri toimijoiden kesken. Työkalu ohjaa osaltaan toimimaan prosessin mukaisesti ja prosessirajapintojen yli. Muutoksenhallinnan ja konfiguraatitiedon ylläpitovastuun asiantuntijalähtöisyys aiheuttaa kuitenkin vaihtelua konfiguraation kontrollin toteutumiseen. Tästä johtuen verkkolaitteiden elinkaaren yhteiskäyttöinen tieto saattaa jäädä kiireessä dokumentoimatta tai vain asiantuntijan omaan käyttöön. Lisäksi vaarana on, että puhelimitse, sähköpostilla tai kollaboraatiotyökaluilla tulevat muutospyynnöt jäävät kirjaamatta. Edellä kuvatun toistuessa konfiguraatitieto rapautuu aiheuttaen luottamusvajetta tietoa kohtaan. Esimerkiksi tietoturva haavoittuvuuksia ei voida arvioida luotettavasti, mikäli tietoon ei voida luottaa.

Nykyinen asiantuntijalähtöinen toimintatapa koetaan pääosiltaan toimivaksi. Kaikki toimijat tietävät oman roolinsa, mutta konfiguraationhallinnan keskitetty johtaminen ja koordinointi koetaan vajaaksi. Esille nousi tarve kuvata tai päivittää ylätasoon prosessi, josta selviää verkkolaitteiden konfiguraationhallinnan vaiheet ja toimijat elinkaaren eri vaiheissa. Lisäksi tärkeänä pidetään muutostöiden loppuun saattamista, ohjeiden noudattamista ja eri toimijoiden jatkuvaa vuoropuhelua myös jatkossa.

Konfiguraation kontrollin ja yhteisen toimintamallin kannalta on tärkeää määritellä mistä tietoverkon verkkolaitteisiin kohdistuvista muutoksista tulee tehdä muutosehdotus (RFC) ja mitkä muutokset voidaan toteuttaa standardimuutoksena. Seuraavassa on lueteltu haastateltavien näkemyksiä molempiin tapauksiin liittyen.

Esimerkkejä muutoksista, joista tulisi laatia muutosehdotus (RFC):

- verkkolaitteiden elinkaarivaihdot.
- yksittäiset laitevaihdot, mikäli aiheuttavat katkoksen verkkoon tai palveluun.
- reititysmuutokset, mikäli aiheuttavat katkoksen verkkoon tai palveluun.
- muut konfiguraation muutokset, mikäli aiheuttavat katkoksen verkkoon tai palveluun.
- kestoltaan pidempi verkon huoltotyö, joka aiheuttaa useita katkoksia verkkoon ja palveluihin.
- vaikutus kohdistuu laajemmin toimintaan, käytettävyyteen tai tietoturvaan.
- uusi ominaisuus, joka otetaan verkossa käyttöön.

Esimerkkejä standardimuutoksista:

- yksittäisen kytkimen vaihto vikatilanteissa ja pienimuotoiset porttimuutokset.
- reitittimien ohjelmistopäivitys perustellusta syystä esim. tiedossa oleva haavoittuvuus.
- muutokset, joissa voidaan soveltaa olemassa olevaa muutoksen vaikutusanalyysiä ja valmiina olevaa fyysistä yhteyttä.
- yksittäiset etähallinnalla tehtävät konfiguraatiomuutokset, joilla ei ole vaikutusta palveluihin.
- muutokset verkon reunalaitteisiin, jotka eivät ole reitittimen tai jakokytkimen tyyppinen solmukohta.
- tapaukset, joissa ei tarvitse rakentaa uutta tai muuttaa konfiguraatiota vaan annetaan käyttöön olemassa olevaa kapasiteettia.
- olemassa olevan käyttöpaikan laajennus.

Muutosten luokittelussa hyödynnetään työnohjaustyökalun tarjoamaa luokittelua, kuten esimerkiksi kiireellisyys, vakavuus ja riski. Monesti käytetään luokittelua, jolla määritetään mihin muutos kohdistuu. Luokittelu voidaan tehdä myös verkon tietoturvaluokan, muutoksen laajuuden ja vaikuttavuuden mukaan.

4.4 Tilan seurannan ja raportoinnin tulosten käsittely

Tilan seuranta ja raportointi tulisi kattaa erityyppisten rakenneosien koko elinkaari. Tilatietojen luokittelussa ei ole yhtä oikeaa mallia. Tarkoituksena on dokumentoida rakenneosien luokittelu niin, että tilaa voidaan seurata. (Bon van 2009, 118.)

Erään haastateltavan mukaan *”kun laite toimii hyvin, niin siinä on muutakin kuin sähköt päällä ja portit ylhäällä”*. Muun muassa tietoturva, käytettävissä oleva kapasiteetti sekä laitteen ja ohjelmiston ikä vaikuttavat loppukäyttäjän asiakaskokemukseen palveluiden käytettävyydestä. Haastateltava painotti, että tilatiedon seurannan lisäksi olennaista on hallita kokonaisuus turvallisesti laitteen koko elinkaaren ajan.

Verkkolaitteiden tilan seurannan ja raportoinnin tarve kohdistuu sähköiseen konfiguraatioon ja itse fyysiseen laitteeseen eli ”rautaan”. Verkon hallintajärjestelmä kerää lokitietoa laitteissa tapahtuvista muutoksista automaattisesti. Tiedon hyödyntäminen vaatii asiantuntijan tekemää louhintaa ja analysointityötä. Laitteen elinkaaren tilatietoa ylläpidetään

muun muassa materiaalinhallinnan tietojärjestelmässä. Myös CMDB-työkalu mahdollistaa tilatiedon ylläpidon, seurannan ja raportoinnin, mikäli laitekannan konfiguraation rakenneosat on tallennettu tietokantaan.

Verkon suunnittelu, verkon valvonta ja hallinta sekä kenttätoiminta kokevat tarpeellisenä laitteen elinkaaren tilatiedon saatavuuden, ylläpidon ja seurannan. Heillä on myös rooli tilatiedon ylläpidossa. Kybertoimijan tarve kohdistuu pääosin automaattisesti saatavaan sähköisen konfiguraation elinkaareen. Tilatiedon tarve on jatkuvaa ja sen ylläpito tulisi tapahtua vain yhdessä paikassa. Laitteen ajantasaisen elinkaaritiedon ylläpito koetaan kuitenkin haastavaksi, koska eri lähteistä ja toimijoilta saatava tieto vaatii myös manuaalista työtä.

Tilatiedon luokittelu tulee olla mahdollisimman yksinkertainen. Verkkolaitteen elinkaaren tilatietoja voivat olla esimerkiksi varastossa, odottaa käyttöönottoa, käytössä, poistettu, poistettu tilapäisesti, vialla ja hylätty. Verkon valvontaa ja hallintaa kiinnostaa milloin laite on aktiivisena verkossa, onko laite verkossa mutta ei aktiivisena tai poistetaanko laite valvontajärjestelmästä. Verkon suunnittelun asiantuntijat sekä kenttätoiminnan asentajat ovat kiinnostuneita laitteiden hankintaan, materiaalinhallintaan ja logistiikkaan liittyvästä tilatiedosta.

Erityinen huomio tulee kiinnittää ajantasaisen tilatiedon saatavuuteen, tilatiedon ylläpidon toimintatapaan ja elinkaarensa päässä olevan laitekannan päivittämiseen riittävän ajoissa. Kokemusten mukaan virheellinen tilatieto aiheuttaa muun muassa turhia vikailmoituksia. Lisäksi verkossa olevat vanhat laitteet lisäävät verkkovikojen ja palvelukustosten todennäköisyyttä merkittävästi. Haastateltavien mukaan käytettävissä olevien järjestelmien ja työkalujen ominaisuudet sekä uusien verkkolaitteiden saatavuus tukevat riittäväällä tavalla edellä kuvattujen perusasioiden toteutumista. Tiedonhallinnan kunnossa olevat perusasiat mahdollistavat myös raportoinnin käyttötärpeen mukaan.

4.5 Prosessien ja roolien tulosten käsittely

Prosessissa luodaan, käsitellään ja muokataan tietoja henkilö- ja organisaatiroolien mukaisesti. Tiedonhallinnan näkökulmasta prosessin jatkuvaan toimintaan nivoutuu erilaisia tietovirtoja. Keskiössä ovat ihmiset, joilla prosessinäkökulman lisäksi on merkittävä tiedon käyttäjän ja ylläpitäjän rooli. (Kaario & Peltola 2008, 69, 137.)

Haastattelussa nousi esiin lausuma, jonka mukaan *”prosessitoimintaa ei ole, ellei sitä ole kuvattu, roolitettu, koulutettu ja jalkautettu”*. Osa haastateltavista kokee, että palveluomaisuuden- ja konfiguraationhallintaprosessi kommunikoi tällä hetkellä häiriöhallinta-, muutoksenhallinta-, ongelmanhallinta- ja palvelupyyntöprosessin kanssa. Osa taas ei tunnista konfiguraationhallintaa omaksi prosessikseen. Tältä osin kaivataan nykyiseen toimintaan sidottua ymmärryksen laajentamista sekä prosessien riippuvuussuhteiden avaamista ja jalkauttamista. Kohdassa ”konfiguraation kontrolli” kuvattu asiantuntijalähtöinen toimintamalli koetaan kehittämistarpeesta huolimatta pääosiltaan toimivaksi. Osin siksi, että CMDB-ominaisuuden sisältävä työnohjaustyökalu ohjaa käytännön tekemistä prosessin mukaisesti ja prosessirajapintojen yli. Työkalua pidetään kantavana voimana edellyttäen, että kaikki sitoutuvat sen käyttöön. Työkalun rinnalla toimii aktiivinen vuoropuhelu eri medioiden välityksellä. Haasteeksi koetaan mahdollisesti roikkumaan tai ilman kohtuullista aikavastetta jäävät tiketit. Syynä voi olla tiketiltä puuttuva olennainen tieto tai tilapäinen resurssivaje. Tikettiä laadittaessa tarpeellista tietoa ei välttämättä ole saatavilla. Puuttuvan tiedon etsiminen saattaa pahimmillaan tuplata työn tekemiseen kuluvan ajan. Esimerkiksi vikatilanteissa tiedon etsimisen aikaviiveet pidentävät palvelun palauttamista. Konfiguraationhallinnan tehtävänä on tarjota tarpeellista tietoa häiriöhallintaprosessille vikatilanteen selvittämiseksi. Tarvittaessa häiriöhallintaprosessi eskaloi vian juurisyyn selvittämisen ongelmanhallintaprosessille, jota konfiguraationhallinnan tulee kyetä edelleen tukemaan.

Konfiguraationhallinta ei ole prosessista tai roolista erillään olevaa työtä, vaan sen tulee sisältyä perustekemiseen. Työtä voidaan verrata dokumentointiin. Työ on valmis vasta, kun dokumentointi on tehty. On hyvä tiedostaa, että sama ihminen voi tehdä työtä useassa prosessissa ja toimia samanaikaisesti eri rooleissa. Vaarana on, että työ henkilöityy ja jakaantuu epätasaisesti. Resurssit huomioiden tämä asettaa vaatimuksia mahdollisimman automaattisesti tuotettavalle konfiguraatietiedolle ja sen ylläpidolle. Prosessivastuuhenkilöiden säännöllisellä yhteydenpidolla voidaan varmistaa, että prosessit keskustelevat keskenään, tekeminen pysyy järkevänä ja että prosessit tuottavat odotettua hyötyä organisaatiolle.

4.6 Yhteenveto ja päätelmät teemahaastattelun tuloksista

Haastattelukutsujen yhteydessä lähetetty kysymysrunko mahdollisti haastateltavien ennakoon tapahtuvan valmistautumisen. Kysymysrunko helpotti asiantuntijoiden orientoitumista varsinaiseen haastatteluun. Tämä oli tarpeellista, koska teemoihin sisältyi myös yksityiskohtiin meneviä kysymyksiä ja konfiguraationhallinnan käsitteitä. Haastattelujen tuotoksena syntyi runsas ja laaja-alainen aineisto. Ennen analysointia ja tulosten kirjoittamista litteroitua aineistoa rajattiin opinnäytetyön tarkoituksen ja tavoitteiden mukaisella tavalla. Rajauksessa huomioitiin aineiston tietoturvaluokan asettamat vaatimukset. Aineiston analyysi ja tulokset esitetään neljästä teemasta, joita ovat konfiguraation tunnistaminen, konfiguraation kontrolli, tilan seuranta ja raportointi sekä prosessit ja roolit.

Teknisen konfiguraatitiedon tunnistaminen, keräys ja ylläpito kohdistuu verkkolaitteiden sähköiseen konfiguraatioon ja itse laitteeseen eli ”rautaan”. Tutkimuksen tuloksista ilmenee, että tietoa hankitaan ja sitä käytetään lähinnä asiantuntijälähtöisesti oman työtehtävän tarpeisiin. Toki tieto palvelee välillisesti myös muita, mutta havaittavissa on roolin tai tehtävänkuvan mukaan tapahtuvaa siiloutumista. Syynä saattaa olla, ettei yksittäinen toimija tunne toimintatavan kokonaisuutta. Seurauksena on tiedon sirpaloituminen, jolloin tietoa ei saada tehokkaasti verkon suunnittelun, ylläpidon tai palvelutuotannon prosessien käyttöön. Useamman haastateltavan mukaan olennaista ei ole yksittäinen tieto, vaan kokonaisuus, josta selviää verkon rakenne ja verkkolaitteiden väliset relaatiot eli suhteet. Relaatioiden tunnistamista pidetään erityisesti korkeamman suojaustason verkoissa tietoturvaan liittyvänä vaatimuksena. Haasteeksi koettiin tiedonsaannin riittävä nopeus ja ajantasaisuus eri tilanteissa. Yksittäisenä ratkaisuna nähtiin verkon valvonta- ja hallintajärjestelmässä olevan tiedon automaattinen siirto palvelunhallintajärjestelmän CMDB-kantaan. Olennaista on määritellä, kuka tietoa käyttää, mitä tietoa halutaan ja miten tieto kyetään ylläpitämään. CMDB-kannan tarpeellisuutta voidaan perustella muun muassa eri toimijoiden yhteisillä tietotarpeilla sekä palvelunhallintajärjestelmän tiketöinnin ja raportoinnin kehittämällä.

Konfiguraation kontrollin tehtävänä on käytännössä varmistaa, että verkkolaitetta koskevat kaikki muutokset toteutetaan ja dokumentoidaan sovitun toimintatavan mukaisesti varaston hyllyltä laitteen hävittämiseen asti. Kontrollioivana työkaluna toimii muutoksenhallintaprosessi. Haastateltavat olivat yksimielisiä keskitetyn muutoksenhallinnan tärkeydestä, vaikka nykyinen toiminta on hyvin asiantuntijälähtöistä. Asiantuntijälähtöisyys ai-

heuttaa vaihtelua konfiguraation kontrollin toteutumiseen. Konfiguraatiomuutosten yhdistävänä tekijänä toimii muun muassa verkon hallintajärjestelmä ja palvelunhallintajärjestelmän tiketöintityökalu. Työkalu ohjaa osaltaan toiminaan prosessin mukaisesti ja prosessirajapintojen yli. Edellä kuvattu toimintamalli koettiin pääosiltaan toimivaksi. Esille nousi kuitenkin tarve kuvata tai päivittää yltäason prosessi, josta selviää verkkolaitteiden konfiguraationhallinnan vaiheet ja toimijat elinkaaren eri vaiheissa. Lisäksi konfiguraation kontrollin ja tekemisen yhtenäisyyden kannalta on tärkeää dokumentoida käytännön esimerkein, mistä tietoverkon verkkolaitteiden muutoksista tulee tehdä muutosehdotus (RFC) ja mitkä muutokset voidaan toteuttaa standardimuutoksena. Esimerkiksi usean verkkolaitteen elinkaarivaihdosta tulisi tehdä muutosehdotus, kun taas yksittäisen kytkimen portin tilamuutos voidaan tehdä standardimuutoksena. Muutoksen luokittelussa voidaan hyödyntää tiketöintityökalun tarjoamaa luokittelua, kuten esimerkiksi laajuus, kiireellisyys, vakavuus tai riski.

Konfiguraation rakenneosien tilatiedon seuranta on yksi lenkki konfiguraationhallinnan kokonaisuuden ketjussa. Tilatiedon luokittelu tulisi tehdä siten, että laitteen tilaa voidaan seurata kaikissa elinkaaren vaiheissa. Tilatiedon luokitteluun ei ole yhtä oikeaa mallia. Yksinkertaisuudessaan tilatietoja voivat olla varastossa, odottaa käyttöönottoa, käytössä, poistettu, poistettu tilapäisesti, vialla ja hylätty. Eri toimijoiden tiedon tarve vaihtelee elinkaaren eri vaiheissa. Ylläpitovaiheessa verkon valvontaa ja hallintaa kiinnostaa verkossa aktiivisena olevat laitteet. Kun laite poistetaan verkosta, tarvitaan lupa sen poistoon valvontajärjestelmästä. Vastaavasti verkon suunnittelun sekä kenttätoiminnan asentajat tarvitsevat materiaalinhallintaan ja logistiikkaan liittyvää tilatietoa erityisesti elinkaaren alku ja loppupäässä. Olennaista on kiinnittää huomiota yhteiskäyttöisen tiedon ylläpidon toimintatapaan ja ajantasaisen tiedon saatavuuteen. Haastattelujen perusteella voidaan todeta, ettei tilatiedon ylläpito ja raportointi jää kiinni käytössä olevista järjestelmistä, työkaluista tai materiaalista. Järjestelmät ja työkalut sisältävät ominaisuuksia, joiden hyödyntämisestä on hyvä pohtia verkkolaitteiden konfiguraationhallintaa kehitettäessä.

Palveluomaisuuden- ja konfiguraationhallinnan sekä muiden prosessien tuottamaa tietovirtaa tulisi kyetä kanavoimaan tehokkaasti tarvitsijoiden käyttöön. Keskiössä ovat ihmiset, joilla prosessinäkökulman lisäksi on merkittävä tiedon käyttäjän ja ylläpitäjän rooli. Osa haastateltavista kokee palveluomaisuuden- ja konfiguraationhallintaprosessin kommunikoivan palveluntuotannon keskeisten tukipalveluprosessien kanssa. Toisaalta osa

haastateltavista ei tunnista konfiguraationhallintaa erillisenä prosessina, vaan se koetaan sisältyvän osaksi nykyistä toimintamallia ja päivittäistä työtä. Lisäksi nykyinen toimintamalli koetaan pääosin toimivaksi, koska eri työkaluja sisältävä palvelunhallintajärjestelmä ohjaa toimimaan prosessin mukaisesti ja prosessirajapintojen yli. Tästä huolimatta kaivataan nykyiseen toimintaan sidottua ymmärryksen laajentamista sekä prosessien riippuvuussuhteiden avaamista ja jalkauttamista. Samalla on mahdollista tunnistaa nykyisen toimintatavan pullonkaulat ja päällekkäistä työtä aiheuttavat kohdat prosesseista. Resurssit huomioiden konfiguraatietieto tulisi saada mahdollisimman ketterästi prosessien ja eri rooleissa toimivien henkilöiden käyttöön. Prosessivastuuhenkilöiden säännöllisellä yhteydenpidolla voidaan varmistaa, että prosessit keskustelevat keskenään, tekeminen pysyy järkevänä ja että prosessit tuottavat odotettua hyötyä organisaatiolle.

Teemahaastattelujen tuloksista ilmenee, että eri rooleissa työskentelevien kokeneiden asiantuntijoiden vastauksissa on enemmän yhdistäviä, kuin toisistaan poikkeavia näkemyksiä. Tämä toistuu johdonmukaisesti jokaisella teema-alueella. Toisistaan poikkeavat näkemykset kohdistuivat enemmän asioiden yksityiskohtiin kuin konfiguraationhallinnan laajempaan viitekehykseen. Tietyt näkemyserot saattoivat johtua myös siitä, että haastateltavat tarkastelivat esitettyjä kysymyksiä painottaen enemmän oman roolin tai tehtävän kuvan näkökulmaa. Pelkistään voidaan kuitenkin todeta, että nykyisellä toimintamallilla verkkolaitteiden konfiguraationhallintaa tehdään asiantuntijälähtöisen ammattimaisesti. Runsaslukuinen haastateltavien joukko oli myös hämmästyttävän yksimielinen konfiguraationhallinnan kehittämistarpeista. Kokonaisuuden kannalta olennaisinta on yhtenäistää asiantuntijälähtöistä toimintatapaa, terävöittää konfiguraationhallinnan ja eri tukiprosessien välistä yhteistoimintaa, sekä parantaa yhteiskäyttöisen konfiguraatietiedon saatavuutta.

4.7 Luotettavuuden arviointi

Laadullisen eli kvalitatiivisen tutkimuksen luotettavuutta arvioidaan kahden pääkäsitteen avulla. Reliabiliteetti tarkoittaa tutkimustulosten toistettavuutta ja validiteetilla tarkoitetaan, että tutkitaan oikeita asioita. Luotettavuuden arvioinnilla pyritään varmistamaan, että saadut tulokset ovat oikeita. Laadullisen tutkimuksen luotettavuuskriteerejä ovat luotettavuus, siirrettävyys, riippuvuus, vahvistettavuus ja saturaatio. (Kananen 2015, 343, 352-355.)

Palveluomaisuuden- ja konfiguraationhallinnan käytännöt ovat luonteeltaan ja lähtökohdiltaan organisaatioriippumattomia. Tutkimuksessa hyödynnettiin kirjallisuus- ja haastattelututkimuksen lisäksi tutkijan omaa yleistä kokemusta IT-toimialalta. Käytetyt tutkimusmenetelmät antoivat samankaltaisia tuloksia, jotka tukivat toisiaan. Edellä kuvattu asetelma antaa hyvän pohjan tutkimusongelmien lähestymiseen ja lisää osaltaan tutkimuksen luotettavuutta. Toisaalta tutkijan omaan kokemukseen perustuvat näkemykset saattavat olla ongelmallisia luotettavuuden kannalta. Täyden objektiivisuuden takaamiseksi tutkijan tulisi olla organisaation ulkopuolinen henkilö, joka ei tunne tutkittavaa asiaa.

Tutkimustyöhön soveltuvaa kirjallista lähdeaineistoa oli tarjolla riittävästi. Lähteiden valinnassa kiinnitettiin huomiota julkaisuajankohtaan. Tutkimuksessa käytettyjen oleellisten lähteiden ikä vaihtelee alle viiden, mutta enintään kymmenen vuoden välillä. Valintaan vaikutti myös tutkimuksen tarkoituksen ja tavoitteiden toiminnallinen sekä tutkimusilmion kehityslähtöinen näkökulma. Konfiguraationhallinnan substanssilähteen kirjoittajasta tai toimittajasta riippumatta niissä viitattiin usein ITIL-viitekehykseen, joka tarjoaa järjestelmällisen lähestymistavan laadukkaiden IT-palveluiden tuottamiseen. Laajasti siteerattu viitekehys kertoo omaa kieltään sen kansainvälisestä suosiosta ja soveltuvuudesta käyttötarkoitukseensa. Osin tästä johtuen käytettyjen lähteiden monipuolisuus jäi hieman vajaaksi. Kaikesta huolimatta asialla saattaa olla tutkimuksen siirrettävyyttä lisäävä vaikutus.

Teemahaastattelujen tulokset ja niiden analysointi perustui sanatarkasti äänitteistä litteoituun aineistoon. Ennen tulosten kirjoittamista ja analysointia aineistoa rajattiin vastaamaan opinnäytetyön tarkoitusta ja tarkentuneita tavoitteita. Lisäksi tutkimus raportoitiin aineistokokonaisuuden julkisuusrajoitukset huomioiden. Näiden osalta tulkinnan luotettavuus ja siirrettävyys eli sovellettavuus voi jäädä vajaaksi. Muilta osin julkisuusrajoitukset eivät rajoita luotettavuuden ja siirrettävyyden arviointia, koska tutkimuksen teoriaosa on laadittu kokonaan julkisista lähteistä. Tutkijan omaan päätökseen perustuen analysoituja tuloksia ei lähetetty haastateltaville luettavaksi. Päätökseen vaikutti opinnäytetyön valmistumisen aikatauluun liittyvät käytännön syyt. Tämä heikentää osin tutkimustulosten vahvistettavuutta vaikka tutkimusaineistoa vertailtiin kirjallisuustutkimuksen aineistoon. Riippuvuus varmistettiin toimeksiantajan ohjaajan avulla. Riippuvuus tarkoittaa, että tulokset on johdettu oikein aineistosta.

Yksilö- ja tiimihaastatteluihin valittiin työn toimeksiantajan organisaatiosta yhteensä viisitoista asiantuntijaa, joita tutkittava ilmiö koskettaa. Asiantuntijoilla oli laaja-alainen ja

vuosien kokemus IT-alan eri tehtävistä. Haastatteluissa kerätty aineisto saavutti kokonaisuuden osalta ennako-odotuksia vahvemman saturaation eli kylläntymisen. Tämä vahvistaa osaltaan tutkimuksen luotettavuutta. Jälkikäteen arvioituna haastateltavien asiantuntijoiden määrä olisi voinut olla pienempi. Toisaalta jokaisen haastateltavan panos oli tutkimuksen kannalta tärkeä. Kaikissa haastattelutapahtumissa nousi esille eri näkökulmia ja yksityiskohtia, jotka auttoivat tutkijaa ymmärtämään tutkittavaa ilmiötä entistä paremmin. Tutkittavan aiheen laajuudesta johtuen työ rajattiin koskemaan organisaation omaa toimintaa. Jatkossa konfiguraationhallinnan muita sidosryhmä- ja kumppanirajapintoja on hyvä tarkastella erikseen tai aihealueen muun kehittämistyöhön yhteydessä.

Yhteenvedona voidaan todeta, että tutkimuksen asiasisältö ja rakenne jäsenyi opinnäytetyön kokonaisuuden edistyessä. Tämä asetti haasteita myös teemahaastattelun kysymysrungon laatimiselle. Tutkimus lopulta osoitti, että alkuperäinen kysymysrunko oli liian laaja. Tämä johtui osiltaan siitä, että tutkija oli määrittänyt tutkimuksen lähtötilanteen tavoitteet liian laajaksi. Tutkimusaineiston rajaus selkeytti tutkimustyön etenemistä. Tutkijan näkemyksen mukaan rajauksella lisättiin tutkimustulosten validiteetin lisäksi myös reliabiliteettia. Tutkija kokee, että edellä kuvatuista asetelmista ja haasteista huolimatta tutkimus on kokonaisuuden osalta dokumentoitu sellaisella tarkkuudella, että saadut tulokset ovat työn tarkoitukseen sekä tavoitteisiin nähden pääosin valideja ja reliaabeleja.

5 EHDOTETUT KEHITTÄMISTOIMENPITEET

Tutkimuksen lähtökohdaksi valittiin käytännön toiminnallisuutta painottava näkökulma. Valintaan vaikutti tutkijan omat havainnot konfiguraationhallinnan yhteensovittamisen haasteista suhteessa muihin IT-palvelutuotannon käytäntöihin. Kvalitatiivisen eli laadullisen tutkimuksen aihealuetta käsiteltiin verkkotekniikan, verkon tietoturva vaatimusten, palvelunhallinnan, tiedonhallinnan, konfiguraation elinkaarenhallinnan, konfiguraationhallintajärjestelmän ja prosessien näkökulmasta.

Toimivia tietoverkkoyhteyksiä ja niiden kautta käytettäviä palveluita pidetään lähes välttämättöminä ja itsestään selvinä hyödykkeinä. Käytännössä loppukäyttäjää kiinnostaa vain toimivat palvelut ajasta ja paikasta riippumatta. Tämä nykypäivän palvelukeskeinen normaali on osaltaan ohjannut IT-alan tekniikan toimijoita päivittämään ajattelun, tekemisen ja toimintatapojen kulttuuria. Toisaalta toimialan omat innovaatiot ja käytännön ratkaisut ovat toimineet muutoksen moottoreina yritysten, erilaisten organisaatioiden ja kansalaisten suuntaan. Edellä kuvattu alan voimakas kehitys ja kasvu on lisännyt myös verkkojen tietoturvaan liittyviä haasteita. Suojaustasosta riippumatta verkkojen perusvaatimukseen kuuluu, että tieto on hallitusti vain valtuutettujen käyttäjien ulottuvilla, muokattavissa ja saatavilla. Nämä vaatimukset tulee huomioida myös palveluomaisuuden ja konfiguraationhallinnan käytäntöjä kehitettäessä.

Parhaiden käytäntöjen soveltaminen

Opinnäytetyön toimeksiantaja soveltaa ITIL-viitekehyksen periaatteita palvelutuotannon tukiprosesseissa. Tästä johtuen tutkimuksessa palveluomaisuuden- ja konfiguraationhallinnan käytäntöjä tarkastellaan muun muassa kyseisiä viitekehyksiä vasten. Viitekehysistä vanhempi painottaa palvelunäkökulman lisäksi elinkaarimalliin perustuvaa prosessinäkökulmaa. Viimeisin julkaisu nostaa jalustalle asiakaskokemusta, arvoja, ideoita ja ketteryyttä. Julkaisu on päivitetty vastaamaan teknologioiden kehittymisen ja digitaalisen murroksen tarpeita. Toimialan kehityspolku on tuonut tullessaan uusia mahdollisuuksia ja vaihtoehtoja, mutta samalla pakottanut eri osapuolia kehittämään omaa toimintaansa. On hyvä tiedostaa, että viitekehykset eivät kumoa toisiaan. Molemmat tarjoavat edelleen soveltuvia käytäntöjä palveluomaisuuden- ja konfiguraationhallinnan kehittä-

mistyöhön. ITIL-käytäntöjen rinnalla kehittämistyössä voidaan tarpeen mukaan hyödyntää prosessijohtamiseen, prosessikehitykseen, laadunhallintaan sekä IT-hallintatapaan liittyviä muita standardeja, viitekehyksiä ja julkaisuja.

Konfiguraationhallinnan asiantuntijälähtöinen toimintatapa

Tutkimuksessa esille noussut asiantuntijälähtöinen toimintatapa on tutkijan oma ilmaisu palveluomaisuuden- ja konfiguraationhallinnan nykyisestä toimintatavasta. Tämä liittyy osaltaan organisoitumisen perusteeseen, joka puolustusvoimien IT-alalla on tyypillisesti linjaorganisaation ja prosessiorganisaation yhdistelmä. Siinä palvelutuotannon toiminnanohjauksen menetelmiä ovat prosessiohjaus ja toimialaohjaus. Toimialaohjausta hyödynnetään toimialan suorassa johtamisessa, ohjauksessa ja koordinoinnissa linjassa erikseen sovittujen pelisääntöjen ja valtuuksien mukaan. Projektiohjausta käytetään, kun tehtävien toteuttaminen vaatii normaalista poikkeavia järjestelyjä. Edellä kuvattua taustaa vasten asiantuntijaorganisaation asiantuntijälähtöisyys on luonteva tapa palvelutuotannon erikoisosaamista vaativien tehtävien toteuttamiseen. Toimintatapa asettaa asiantuntijoille merkittäviä vastuita. Organisaation palvelutuotannon kannalta on tärkeää, että kaikki sitoutuvat toimimaan prosessien mukaisesti ja käyttämään palvelutuotannon edellyttämiä työkaluja. Sitoutumisen ja muiden kehityskohteiden yhteisvaikutuksella voidaan parantaa pääosin toimivaksi koettua asiantuntijälähtöisen toimintatavan yhtenäisyyttä entisestään. Onnistuakseen tehtävissään asiantuntijat tarvitsevat esimiesten ja organisaation johdon jatkuvan tuen.

Verkkolaitteen elinkaaren hallinta ja konfiguraation rakenneosien luokittelu

Teemahaastatteluissa tietoverkon verkkolaitteita käsiteltiin kokonaisuutena kohdentuen tarkemmin verkon kytkimiin ja reitittämiin. Elinkaarenhallinnan lähtökohtana on, että konfiguraation rakenneosat (CI) ja attribuuttitiedot tunnistetaan ja dokumentoidaan. Kytkin- ja reititintietojen ylläpito on rationaalisinta kytkeä fyysisen laitteen eli ”raudan” elinkaaren vaiheisiin. Elinkaari alkaa laitteen hankinnasta ja päättyy, kun laite poistetaan verkosta ja hylätään. Tämä koskee myös sähköisen konfiguraation tilatiedon muutoksia. Konfiguraatiotasojen määrä kannattaa miettiä huolellisesti. Mitä enemmän tasoja, sitä enemmän ylläpitotyötä. Vähemmän tasoja tarkoittaa käytännössä pienempää tietomäärää. Liian

suppea tietomäärä saattaa vaikeuttaa laitteen elinkaaren hallintaa ja hidastaa vikatilanteissa palvelun palauttamista. Edellä kuvattu toimintamalli tuottaa yhteiskäyttöistä tietoa, jota voidaan hyödyntää muun muassa verkkojen suunnittelussa, verkon valvonnassa ja hallinnassa sekä asennustyössä.

Haastattelujen perusteella taulukkoon 2 on listattu tietoverkkoon tai verkkolaitteisiin liittyviä konfiguraatiotietoja. Taulukosta voidaan valita kytkimen ja reitittimen elinkaaren kontrolliin tarvittavat keskeisimmät rakenneosat ja attribuutit. Valinnan jälkeen luokittelun tasoja syvennetään, sekä nimeämistä ja mahdollisia relaatioita tarkennetaan tarpeen mukaan. Luokittelulla selkeytetään rakenneosien käsittelyä ja raportointia. Dokumentointi kannattaa toteuttaa siten, että halutut tiedot voidaan viedä sellaisenaan konfiguraatietietokantaan (CMDB). Kannassa olevan tiedon ylläpitoa voidaan selkeyttää määrittämällä tietojen omistajuus ja niiden ylläpitovastuut. Samalla vastuut kannattaa sitoa osaksi muita palvelutuotannon prosesseja. Lähtökohtana voidaan pitää, että tiedon ylläpitäjät vastaavat tietojen laadusta niiden omistajalle. Tietojen ylläpito on järkevintä antaa ihmisille, jotka tehtävään, prosessiin tai rooliin liittyen asiasta parhaiten tietävät.

Konfiguraatietiedon ylläpito ja saatavuus

Konfiguraatietietokantaan (CMDB) on mahdollista linkittää tietoja useista tietolähteistä. Tietokanta tarjoaa tiedot keskitetysti eri toimijoiden ja prosessien käyttöön esimerkiksi palvelunhallintajärjestelmän tiketöintityökalun kautta. Kannasta tiketille nostettava tieto yhtenäistää ja parantaa tiedon tarkkuutta. Työkalu mahdollistaa myös raportoinnin. Toimiva keskitetty malli vähentää päällekkäistä työtä sekä poistaa jaettavan tiedon ja moninkertaisen ylläpidon ongelman. Lisäksi tietokannan rakenne dokumentoi palveluiden ja niiden komponenttien loogisen mallin määritetyn tasorakenteen mukaisesti. Ylläpidettävät rakenteet relaatioineen ovat konfiguraatietietokannan ominaisuuksia, jotka lopulta erottavat sen perinteisestä materiaalikirjanpidon tietojärjestelmästä.

Konfiguraatietietojen ylläpito CMDB-kannassa voidaan toteuttaa joko automaattisesti tai manuaalisesti. Automatisointi ei välttämättä ole kytkimiin ja reitittämiin liittyvien kaikkien tietojen osalta tarpeellista, hyödyllistä tai edes mahdollista. On tärkeää tunnistaa kuka tietoa käyttää, mitä tietoa tarvitaan ja mitä tietoa kyetään ylläpitämään. Toteutustavan valinnassa kannattaa huomioida käytössä olevat järjestelmät, kustannukset ja muut resurssikysymykset. Peruslähtökohtana voidaan pitää mahdollisimman automatisoitua ratkaisua. Asiantuntijoiden mukaan tietointegraatio CMDB-kannan sekä automaattisten

verkon valvonta- ja hallintajärjestelmien välillä on teknisesti toteutettavissa kohtuullisin ponnisteluin, ellei muita rajoitteita ole tiedossa. Mahdollisimman automatisoitu ratkaisu säästää resursseja sekä varmistaa paremmin, että tieto on oikeaa ja ajantasaista. Kokonaisvaltaista automatisointia ei voida pitää itsestään selvänä ja ainoana vaihtoehtona. Tarvittaessa toiminta voidaan jakaa automaattisesti ja manuaalisesti ylläpidettäviin konfiguraatietietokannan tietoihin. Nopean muutostiheyden omaavat tilatiedot pyritään automatisoimaan. Manuaalisesti voidaan ylläpitää ne tiedot, jotka eivät laitteen elinkaaren aikana muutu tai muutostiheys on pieni. Automatisoitu käytäntö tarkoittaa, että verkon valvonta- ja hallintajärjestelmä päivittää valitut tiedot automaattisesti konfiguraatietietokantaan joko reaaliaikaisesti tai määrättyinä vuorokauden aikana.

Prosessien välinen yhteistoiminta ja tietovirrat

Tutkimuksessa havaittiin, että toimiva muutoksenhallintaprosessi on konfiguraationhallinnan yksi tärkeimmistä tukiprosesseista. Muutoksenhallinnan tehtävänä on kontrolloida, että verkkolaitteen rakenneosatiedon muutokset tehdään ja dokumentoidaan hallitusti laitteen elinkaaren kaikissa vaiheissa. Mitä parempi on muutoksenhallintaprosessin kypsyys, sitä paremmin ja ketterämmin se kykenee käsittelemään konfiguraatioihin kohdistuvia muutoksia. Tämän raportin kohdassa 4.3 ”konfiguraation kontrolli” luetellaan esimerkkejä verkkolaitteisiin kohdistuvista muutoksista. Luettelossa muutokset jaetaan standardimuutoksiin ja muutoksiin, joista tulee laatia muutospyyntö (RFC). Sopivalla tarkkuudella tehty ja jalkautettu muutosten luokittelu sekä vakiointi nopeuttaa muutosten käsittelyä prosessien tietovirrassa.

Erilaisia työkaluja sisältävä palvelunhallintajärjestelmä ohjaa ihmisiä toimimaan prosessien mukaisesti ja prosessirajapintojen yli. Konfiguraationhallinnan kannalta on tärkeää sitoa rakenneosatietojen ylläpito osaksi prosesseissa käsiteltävää tietovirtaa. Koska työkalu ohjaa toimimaan prosessien mukaisesti, on luontevaa käsitellä ja ylläpitää laitteen elinkaaren yhteiskäyttöisiä konfiguraatietietoja samalla työkalulla. Lähtökohtana on, että työkaluun sisältyy CMDB-tietokanta ja sitä käytetään. Tämä mahdollistaa tiketöintityökalun tikettien kuljettaman tietovirran prosessien sisällä ja prosessirajapintojen yli. Halutun toimintatavan kokonaisuuden kuvaus ja jalkauttaminen yhtenäistää verkkolaitteiden konfiguraationhallintaa entisestään sekä antaa merkittävää lisäarvoa IT-organisaation palvelutuotantoon. Lisäksi prosessivastuuhenkilöiden säännöllisellä yhteydenpidolla huo-

lehditaan, että prosessit keskustelevat keskenään ja konfiguraationhallinnan kokonaisuudesta voidaan raportoida ajantasaista tilannekuvaa. Samalla varmistetaan, että konfiguraationhallinta tuottaa odotettua hyötyä muille prosesseille ja koko organisaatiolle.

Lopuksi

Tietoverkon palveluomaisuuden- ja konfiguraationhallinnan yksi tärkeistä tukipilareista on toimiva tiedonhallinta. Teoriaosan kuvassa 7 esitetyn tiedonhallinnan viitekehyksen osia ovat roolit, prosessit, tiedot ja teknologia. Tämä tutkimus osoittaa, että näiden osien keskinäinen yhteistoiminta ja tasapaino vaikuttavat merkittävästi palveluomaisuuden- ja konfiguraationhallinnan suorituskykyyn.

Tutkimuksessa selvitettiin, miten verkkolaitteiden palveluomaisuuden- ja konfiguraationhallintaa voidaan toiminnallisesti kehittää perinteisissä tietoverkoissa. Tästä lähtökohdasta katsoen voidaan todeta, että työ on saavuttanut sille asetetut tavoitteet. Konfiguraationhallintaa kannattaa tutkia myös jatkossa, koska IT-ala digitalisoituu entisestään robotiikan ja tekoälyn yleistyessä. Jatkotutkimuksen aihe voisi liittyä uuden sukupolven verkkojen ohjelmisto-ohjattuun SDN-tekniikkaan (Software Defined Networking). Tutkimuksella voisi selvittää, miten automatisoituva tietoverkkojen konfiguraationhallinta vaikuttaa edellä mainitun tiedonhallinnan viitekehyksen dynamiikkaan ja mitä osa-alueita verkkojen konfiguraationhallinnasta joudutaan myös jatkossa tekemään manuaalisesti.

LÄHTEET

- Ahmad, I. 2018. Improving software defined cognitive and secure networking. University of Oulu. Tampere: Juvenes Print. Viitattu 27.04.2020 <http://jultika.oulu.fi/Record/isbn978-952-62-1951-6>
- Beasley, JS. & Nilkaew, P. 2012. Networking Essentials, Third edition. Indianapolis: Pearson education, Inc.
- BMC Software 2016. Step-by-Step Guide to Building A CMDB. Third edition. BMC Software.
- Bon van, J. 2009. ITIL® V3 - Taskukirja. Amersfoort: Van Haren Publishing. Suomenkielinen painos. Helsinki: Kyriiri Oy.
- Cisco Networking Academy 2018. Scaling Networks v6. Companion Guide. Indianapolis: Cisco Press.
- Drogseth, D.; Strum, R. & Twin, D. 2015. CMDB Systems: Making Change Work in the Age of Cloud and Agile. Amsterdam: Elsevier, Inc.
- Froom, R. & Frahim. E. 2015. Implementing Cisco IP Switched Networks (SWITCH). Foundation Learning Guide. Indianapolis: Cisco Press.
- Hirsjärvi, S.; Remes, P. & Sajavaara, 2015. Tutki ja kirjoita. 15. painos. Helsinki: Tammi.
- ITIL Foundation. ITIL 4 Edition 2019. London: The Stationery Office.
- ITIL Perustason käsikirja 2013. London: The Stationery Office.
- ITIL Service Strategy 2011. London: The Stationery Office.
- Julkisen hallinnon tietohallinnon neuvottelukunta – JUHTA 2019. JHS 212 ICT-palvelujen palvelutasonhallinta (SLM). Viitattu 22.5.2020 <http://docs.jhs-suositukset.fi/jhs-suositukset/JHS212/JHS212.pdf>
- Kaario, K. & Peltola, T. 2008. Tiedonhallinta. Avain tietotyön tuottavuuteen. Porvoo: Bookwell
- Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylän ammattikorkeakoulun julkaisuja 202. Suomen Yliopistopaino Oy – Juvenes Print.
- Kosola, J. 2013. Vaatimustenhallinnan opas. Maanpuolustuskorkeakoulu, Sotatekniikan laitos. Julkaisusarja 5 No 12. Tampere: Juvenes Print.
- Lönngvist, A.; Blomqvist, K. Hannula, M., Kianto, A., Kärkkäinen, H., Maula, M. & Ståhle, P. 2007. Tietojohtaminen tutkimusalueena. Tampere: Pilot-kustannus Oy.
- Peltoniemi, L. 2019. ITIL 4 – Uusimmat uutiset. Webinaari 15.2.2019. Wakaru Oy. Viitattu 25.3.2019 <https://www.oppia.fi/webinars/itil4uutisia#info>
- Puolustusvoimat 2020. Puolustusvoimien johtamisjärjestelmäkeskus. Viitattu 4.4.2020 <https://puolustusvoimat.fi/tietoa-meista/johtamisjarjestelmakeskus>
- Pääesikunta 2017 ja 2019. Päätökset Tapio Pulkkinen tutkimuslupahakemukseen (AN12143 ja AP4059). Viitattu 23.4.2020.
- SFS-ISO/IEC 20000-1. 2018. Informaatioteknologia. Palvelunhallinta. Osa 1: Palvelunhallintajärjestelmää koskevat vaatimukset., 2. painos Helsinki: Suomen Standardisoimisliitto SFS ry.

SFS-ISO/IEC 20000-2. 2014. Informaatioteknologia. Palvelunhallinta. Osa 2: Ohjeistusta palvelunhallintajärjestelmän toteuttamiseen. Helsinki: Suomen Standardisoimisliitto SFS ry.

SFS-ISO/IEC 20000-10. 2018. Informaatioteknologia. Palvelunhallinta. Osa 10: Käsitteet ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS ry.

Shirley, L. & Norfolk, D. 2014. Configuration Management: Expert guidance for IT service managers and practitioners, Revised edition. United Kindom, Swindon: BCS Learnig and Development Ltd.

Suurla, R. 2001. Avauksia tietämyksen hallintaan. Eduskunnan kanslian julkaisu 1/2001. Helsinki: Oy Edita Ab.

Sääksvuori, A. & Immonen, A. 2002. Tuotetiedonhallinta PDM. Jyväskylä: Gummerus.

Sydänmaalakka, P. 2013. Älykäs johtaminen 7.0. Miten kasvaa viisaaksi johtajaksi? Helsinki: Talentum.

Valtionhallinnon tietoturvallisuuden johtoryhmä 2010. Sisäverkko-ohje, VAHTI 3/2010.

Valtionvarainministeriön julkaisuja 2020:19. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Viitattu 22.5.2020 <https://julkaisut.valtioneuvosto.fi/handle/10024/162154>

Viestintävirasto 54 B/2014 M. Määräys viestintäverkkojen ja -palveluiden varmistamisesta sekä viestintäverkkojen synkronoinnista. Viitattu 22.5.2020 <https://www.traficom.fi/fi/saadokset?group=viestintäverkot&limit=50&offset=0&query=Määräys%2054&sort=created>

Teemahaastattelun kysymysrunko

Konfiguraation tunnistaminen

- Tunnettaanko organisaatiossa peruskäsitteet? (rakenneos, attribuutti, relaatio, konfiguraatietietue, perustaso)
- Kuvaile konfiguraation tunnistamisen toimintatapa tällä hetkellä?
- Mitä konfiguraation rakenneosien tietoja kerätään, luokitellaan ja ylläpidetään?
- Onko perustasot tunnistettu ja määrä sopiva? Jos määrä ei ole sopiva, niin mitä pitäisi lisätä tai poistaa?
- Onko viimeisin perustason informaatio helposti tarvitsijoiden käytettävissä?
- Pyritäänkö kaikki konfiguraation rakenneosien rajapinnat/relaatiot tunnistamaan?
- Verkon valvonta- ja hallintajärjestelmä kerää verkkolaitteista automaattisesti tietoa valtavan määrän. Mitä näistä tiedoista tulisi siirtää ja ylläpitää konfiguraatio-tietokannassa (CMDB)?

Konfiguraation kontrolli (lisäys, muutos, vaihto ja poisto)

- Noudatetaanko muutoksenhallinnan periaatteita käytännössä? Jos ei, niin miksi ei?
- Onko muutokset luokiteltu ja millainen luokittelu voisi olla hyvä?
- Minkälaisista muutoksista pitäisi tehdä muutosehdotus (RFC)? Miksi?
- Minkälaiset muutokset voidaan toteuttaa standardimuutoksina? Miksi?
- Kuka käsittelee ja arvioi muutokset sekä niiden vaikutukset? Kuka päättää muutoksen tai jakelun toimeenpanon?

Tilan seuranta ja raportointi (tiedon hallinta)

- Onko tilatiedot määritelty ja millainen määrittely voisi olla hyvä?
- Onko konfiguraatietiedon ylläpitovastuut/roolit jaettu tai miten vastuut olisi hyvä jakaa?
- Kenen tarpeita tiedonkeruu ja tilatiedon ylläpito tulisi palvella?
- Mitä tietoliikenneverkkolaitteiden konfiguraatietietoa omassa työssäsi tarvitset?
- Saatko työsi kannalta tarpeellisen konfiguraatietiedon helposti käyttöön? Onko tieto ajantasaista?
- Tukeeko työkalut ja järjestelmät riittävällä tavalla elinkaaren eri vaiheiden tilatiedon ylläpitoa ja raportointia ja laajemmin palveluomaisuuden- ja konfiguraation-hallintaa?

Prosessit ja roolit

- Palveluomaisuuden- ja konfiguraationhallinta liittyy kaikkiin palvelun elinkaaren prosesseihin: Kuinka hyvin mielestäsi palveluomaisuuden- ja konfiguraationhallintaprosessi kommunikoi tällä hetkellä esimerkiksi häiriönhallinta-, muutoksenhallinta-, ongelmanhallinta- ja palvelupyyntöprosessin kanssa?
- Miten prosessien ja eri roolien välinen kommunikointi käytännössä toimii?